



ربيع الأخر ١٤٣٥هـ/ فبراير ٢٠١٤م

مجلة فصلية تصدرها مدينة الملك عبدالعزيز للعلوم والتقنية

السنة (٢٨) العدد (١١٠)

تقنية الإلكترونيات

النظم الرقمية ص ٣

الهواتف المحمولة الذكـيــة ص ٣١

ISSN 1017 3056

www.kacst.edu.sa

المراسلات

مدينة الملك عبدالعزيز للعلوم والتقنية
الإدارة العامة للتوعية العلمية والنشر
ص ب ٦٠٨٦ ـ رمز بريدي ١١٤٤٢ ـ الرياض
هاتف ٤٨٨٣٥٥٥ ـ فاكس ٤٨١٣٣١٣

Journal of Science & Technology
King Abdulaziz City For Science & Technology
Gen. Direct. of Sc. Awa. & Publ. P.O. Box 6086
Riyadh 11442 Saudi Arabia

jscitech@kacst.edu.sa
www.kacst.edu.sa



رادارات الاستطلاع الثانوية ١٨



مصفوفة الهوائيات المُضَعّفة ٢٤



تشفيـر المعلـومـــات ٢٨

منهــاج النشـــر

أعزاءنا القراء:

يسرنا أن نؤكد على أن المجلة تفتح أبوابها لمساهماتكم العلمية واستقبال مقالاتكم على أن تراعى الشروط التالية في أي مقال يرسل إلى المجلة:

- يكون المقال بلغة علمية سهلة بشرط ألا يفقد صفته العلمية بحيث يشتمل على مفاهيم علمية وتطبيقاتها.
- أن يكون المقال ذا عنوان واضح ومشوّق ويعطي مدلولاً على محتوى المقال.
- في حالة الاقتباس من أي مرجع سواء كان اقتباساً كلياً أو جزئياً أو أخذ فكرة يجب الإشارة إلى ذلك ، وتذكر المراجع لأي اقتباس في نهاية المقال.
- ألا يقل المقال عن ثمانِ صفحات ولايزيد عن أربع عشرة صفحة مطبوعة، وفي حدود من ٢٠٠٠ إلى ٣٥٠٠ كلمة.
- أن يكون المقال أصيلاً ولم يسبق نشره في مجلات أخرى.
- إرفاق أصل الرسومات والصور والنماذج والأشكال المتعلقة بالمقال .
- المقالات التي لاتقبل النشر لاتعاد لكاتبها.
- يمنح صاحب المقال المنشور مكافأة مالية من ١٠٠٠ إلى ٢٤٠٠ ريال .

يمكن الاقتباس من المجلة بشرط ذكر اسمها مصدراً للمادة المقتبسة

الموضوعات المنشورة تعبر عن رأي كاتبها



محتويات العدد

المركز الوطني للإلكترونيات والاتصالات والضوئيات	٢
النظم الرقمية	٤
شبكة الهاتف العامة	٨
عالم في سطور	١٣
الهواتف المحمولة الذكية	١٤
رادارات الاستطلاع الثانوية	١٨
مصفوفة الهوائيات المُضَعّفة	٢٤
تشفير المعلومات	٢٨
أجهزة التشفير.. هل تحمينا؟	٣٤
المُحتَوَى الإلكترونيّ لطبقة الأيونوسفير	٤٠
الإبداع في بيئة العمل البحثية	٤٤
عرض كتاب	٤٨
كيف تعمل الأشياء	٥٢
بحوث علمية	٥٥
مصطلحات علمية	٥٦
من أجل فلذات أكبادنا	٥٧
الجديد في العلوم والتقنية	٥٨

كلمة التحرير

قراءنا الأعزاء

هانحن نطل عليكم في عدد جديد وموضوع شيّق وجّذاب نأمل أن يحوز على رضاكم واستحسانكم؛ فقد عاهدنا أنفسنا على مواصلة الجهد الدؤوب والحثيث للوصول بالمجلة إلى أعلى مستويات الدقّة العلمية والتنويع المتجدد في موضوعاتها حرصاً منّا على ميول القرّاء المختلفة، وفي هذا العدد نتناول موضوعاً مهماً في حياتنا اليومية وهو عن الإلكترونيات لأنها تَشغُل حيزاً كبيراً من حياتنا اليومية المعاصرة حيث أصبحت عصب الحياة.

تناول العدد موضوعات عديدة مهمة عن تقنية الإلكترونيات من عدة جوانب مثل : النظم الرقمية وكيف دخلت تقنياتها إلى حياتنا اليومية لتصبح أصغر حجماً وأفضل أداء وأقل ثمناً من السابق، وكذلك شبكة الهاتف العامة الذي تناول اختراع الهاتف ووظيفته وتطوره وتقنيات المقاسم الهاتفية، كما تناول العدد الهواتف المحمولة الذكية، متطرقاً إلى أمثلة ومزايا الأجهزة الذكية ومكونات النظام في شريحة. كما تناول العدد رادارات الاستطلاع الثانوية من حيث مكوناتها واستخداماتها، إضافة إلى مصفوفة الهوائيات المضعفة وكيفية عملها، وقد تطرق العدد - أيضاً - إلى تشفير المعلومات وكيف كان التشفير في العصور القديمة والعصر الحديث، واستعرض وحدة التشفير وطرق الحماية من الهجمات على أجهزة هذه الوحدات وأنواع هذه الهجمات. وأخيراً فقد تناول العدد المحتوى الإلكتروني لطبقة الأيونوسفير وتأثيرها على الاتصالات اللاسلكية وحساب المحتوى الإلكتروني لهذه الطبقة بالمملكة، بالإضافة إلى العديد من الأبواب الثابتة .

نأمل أن نكون قد وفّقنا في هذا العدد لإرضاء قرّاءنا الأعزّاء في الإحاطة بهذا الموضوع وأن نكون عند حسن ظنهم واستحسانهم، ونتطلع دوماً إلى بذل المزيد من العطاء المتواصل في كل عدد حتى تخرج المجلة في أبهى حلة ، وحتى نكون قريبين دوماً من قراءنا الأعزاء في مختلف أرجاء وطننا العربي الكبير.

والله من وراء القصد،،،

رئيس التحرير

المركز الوطني للإلكترونيات والاتصالات والضوئيات



د. حاتم محمد البحيري، د. محمد سليمان بن صالح، عبدالله عبدالرحمن العثمان

تعد تقنية الإلكترونيات والاتصالات والضوئيات ركيزة من ركائز الاقتصاد القائم على المعرفة، وأساس تبادل المعلومات؛ مما يجعلها ذات أهمية بالغة بالنسبة لسيادة الدول واكتفائها الذاتي. كما تمثل هذه التقنية وسيلة من وسائل تنويع الاقتصاد السعودي -القائم بصفة أساس على الموارد الطبيعية- وإيجاد فرص عمل ذات أجور مناسبة لمتطلبات المواطن السعودي. ونظراً لأهمية هذه التقنية بالنسبة للمملكة، فقد تمّ إدراجها ضمن الخطة الوطنية للعلوم والتقنية والابتكار، التي أقرّها مجلس الوزراء في عام ١٤٢٣هـ / ٢٠٠٢م ضمن برامج التقنيات الإستراتيجية ذات الأهمية الحيوية لتحقيق التنمية في المستقبل.

تأسس المركز الوطني للإلكترونيات والاتصالات والضوئيات في عام ١٤٢٥هـ/٢٠٠٤م لمواكبة الثورة الهائلة في هذا المجال وأخذ زمام المبادرة من قبل **مدينة الملك عبدالعزيز للعلوم والتقنية** للاضطلاع بدورها في دعم وتنسيق الجهود البحثية من خلال بناء شراكات بحثية مع الجامعات ومعاهد البحوث سواء المحلية أو العالمية. وتتركز أهداف المركز الرئيسة في إيجاد بيئة بحثية متكاملة تكون فاعلة في تبني وتطوير حلول تقنية مبتكرة للمتطلبات الاستراتيجية المحلية والعالمية من خلال:

- بناء مختبرات وطنية متخصصة وتجهيزها بأحدث ما توصلت إليه التقنية مع تدريب وتأهيل الكوادر البشرية الوطنية لتشغيل وتطوير تلك المعامل من باحثين ومهندسين وتنمية خبراتهم ومهاراتهم من خلال إشراكهم في مشاريع بحثية متقدمة مع شركاء عالميين متخصصين.
- تطوير نماذج مختبرية وبراءات اختراع لأنظمة وحلول يمكن تطويرها كي تكون منتجات لدفع عجلة وبناء الصناعة في هذا المجال بالمملكة العربية السعودية.
- تبنّى المركز العديد من العمليات والمعايير العالمية في مباشرة مشاريعه البحثية وعملياته اليومية مما يمهد للمضي قدماً في طريق النجاح.

المبادرات والتقنيات المختارة

تم تصنيف أوجه نشاط المركز إلى نوعين هما:

- **مبادرات**

تشير المبادرات إلى مختلف مجالات التطبيقات المتعلقة بتخصصات تقنية محددة، وقد تم اختيارها وفقاً لمعايير اختيار محددة - مستخلصة من السياسة الوطنية للعلوم والتقنية والابتكار- استناداً إلى ثلاثة أنواع من آثار المبادرة أو التقنية وهي: الأثر الاستراتيجي، والأثر الاقتصادي، والأثر العلمي؛ وتم تحديد أربع مبادرات هي:

١- تطوير أجهزة أمن المعلومات.
٢- الاتصالات وشبكات المجسات اللاسلكية.
٣- الليزر وتطبيقاته.
٤-المجسات ومحركات المنظومات الإلكتروميكانيكية المجهرية المتقدمة.

- **تقنيات**

تشير التقنيات إلى مجالات تقنية محددة تخدم العديد من المبادرات، وقد تم اختيار ست تقنيات للمركز هي:

١- الدوائر المتكاملة.
٢- أنظمة الميكروويف.
٣- الحوسبة القابلة للتشكيل.
٤- تصميم وتصنيع ألواح الدوائر المطبوعة.
٥- البصريات الكهربائية.
٦- معالجة الإشارات الرقمية.

الأهداف الاستراتيجية للمركز

حُددت ثمانية أهداف استراتيجية للمركز بما يوائم أهداف وغايات السياسة الوطنية للعلوم والتقنية والابتكار بالمملكة، وتتمثل هذه الأهداف في الآتي:

- نقل وتوطين تقنيات ذات قيمة مضافة عالية.
- تكوين حلقة وصل بين جميع الشركاء و المستفيدين في هذا المجال.
- بناء مختبرات تقنية متقدمة.
- تشجيع الأبحاث العلمية التطبيقية.
- تطوير المناهج التدريبية والتأهيلية.
- تدريب وتأهيل الكوادر الوطنية المتخصصة.
- فتح مجالات استثمارية وتسويقية.
- خلق فرص وظيفية للمتخصصين.

الإنجــــازات

تمثلت إنجازات المركز – تنفيذا لأهدافه الاستراتيجية المذكورة أعلاه - في الآتي:

- **مشاريع بحثية**

يقوم الباحثون في المركز بتنفيذ عدد من المشاريع البحثية، وذلك على النحو الآتي:

- تنفيذ مشاريع تقنية بالتعاون مع شركاء محليين وعالميين، مثل: جامعة الملك فهد للبترول والمعادن، وجامعة الملك سعود، وجامعة الملك عبدالله، ووزارتي الداخلية والدفاع، ويوضح الشكل (١) عدد المشاريع المنفذة من عام ٢٠٠٨ إلى عام ٢٠١٣م.
- تنفيذ العديد من المشاريع لصالح عدد من الإدارات الحكومية والوزارات لتحقيق متطلباتهم البحثية بالتعاون مع القطاع الخاص بالمملكة.
- تنفيذ العديد من المشاريع البحثية التطبيقية التي انتهت إلى نماذج مختبرية جربت في بيئات عملية لحل مشاكل قائمة، مع عرض نتائجها للتبنّي من قبل القطاع الخاص لتسويقها وإنتاجها بكميات تجارية.

- **بناء مختبرات تقنية متقدمة**

أنشأت المدينة عدة مختبرات تقنية حديثة



■ شكل (١) عدد المشاريع المنفذة من عام ٢٠٠٨ إلى عام ٢٠١٣م.



■ مختبر تصنيع الألواح الإلكترونية.

للمساهمة في إنجاز العديد من المشروعات البحثية القائمة بالمركز، من أحدثها ما يأتي:

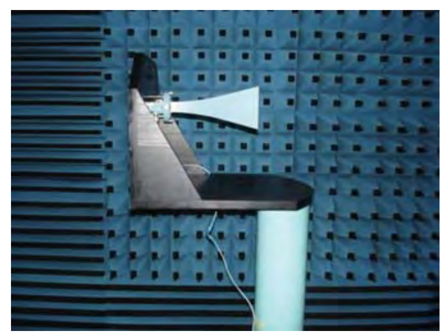
■ مختبر تصنيع الألواح الإلكترونية ويستخدم في:

– تجميع أنظمة الاتصالات والإلكترونيات الحديثة

– تصنيع الألواح الإلكترونية بأعلى المواصفات العالمية، مع طاقة تصنيع منخفضة.

■ مختبر اختبار الهوائيات، وهو عبارة عن غرفة عديمة الارتداد تستخدم في عدة تطبيقات هي:

– فحص خصائص هوائيات ذات أبعاد تصل إلى ٢ م باستخدام برامج حاسوبية وأجهزة تحرك ميكانيكية دقيقة، ٣٦٠ درجة أفقيا، و ٤٥ درجة رأسيا.



■ مختبر اختبار الهوائيات.



■ شكل (٢) نظام تأمين التعاملات الإلكترونية.

– تصميم وتطوير الهوائيات

– تقييم ومعايرة أنظمة الهوائيات المختلفة وإصدار شهادة بيانات موثقة.

– التدريب على فحص واختبار الهوائيات.

■ المشاركة في إعداد السياسات الوطنية في المجالات ذات العلاقة.

● التوظيف والتدريب

قام المركز بتوظيف واستقطاب عدد من الكوادر الوطنية السعودية وتدريبهم على العمل وذلك كما يأتي:

■ المشاركة في تحديث المناهج التدريبية لعدد من الجهات الحكومية.

■ زيادة عدد منسوبي المركز من ٥ موظفين في عام ٢٠٠٤م إلى ١٩٤ موظف بنهاية عام ٢٠١٣م، مع استقطاب خريجي الجامعات السعودية والعالمية السعوديين وإشراكهم في مشاريع نقل التقنية الاستراتيجية، والتي من ضمن أهدافها التدريب على رأس العمل للكوادر السعودية، مما يسهم في توفير كفاءات وطنية مدربة على أعلى المستويات للمشاركة في بناء الصناعة في المملكة.

■ التنسيق مع الجامعات السعودية بتدريب الطلبة خلال الفصل الصيفي والإشراف من قِبل الباحثين بالمركز على مشاريع التخرج للطلبة بإشراكهم في مشاريع ونشاطات المركز.



■ شكل (٣) نظام تأمين أنظمة الحاسب.

■ استقطاب العديد من المتخصصين سواء من القطاع الخاص أو من خريجي برنامج خادم الحرمين الشريفين للابتعاث الخارجي، بالإضافة إلى منسوبي المركز الذين تم ابتعاثهم للعمل في مشاريع تقنية متقدمة.

● جوائز وشهادات

حصل المركز على جائزة المراعي للإبداع العلمي – فرع الوحدة البحثية لعام ٢٠١٢م، وعلى شهادة الجودة (ISO ٩٠٠٢:٢٠٠٨).

● مخرجات علمية

حقق منسوبو المركز العديد من المخرجات العلمية المهمة من خلال تنفيذ خطط المركز الاستراتيجية والتشغيلية وتنفيذ المشاريع البحثية، وتتمثل هذه المخرجات في الآتي:

– تطوير العديد من الأنظمة الإلكترونية الفريدة التي تفتح مجالات استثمارية للقطاع الخاص لإنتاجها وتسويقها ،شكلي (٢)، (٣).

– تقديم العديد من الاستشارات والدعم الفني للعديد من الجهات الحكومية والخاصة من قِبل المختصين بالمركز.

– نشر ١٣ ورقة علمية محكمة في مجلات عالمية ذات مستوى وتصنيف عالمي.

– نشر ٥٨ ورقة علمية في مؤتمرات دولية.

– الحصول على أربع براءات اختراع من مكتب تسجيل براءات الاختراع الأمريكي.

– تنظيم وعقد ثلاثة مؤتمرات بالتعاون مع جمعية مهندسي الإلكترونيات والكهرباء الدولية (IEEE) بالمركز في الأعوام ٢٠٠٩م و٢٠١١م و ٢٠١٣م.

المراجع

– الخطة الوطنية للعلوم والتقنية والانتكار (موقع مدينة الملك عبدالعزيز للعلوم والتقنية).

– الأولويات الاستراتيجية لتقنية الإلكترونيات والاتصالات والضوئيات، المؤتمر الدولي الثاني للتقنيات المتقدمة، الرياض نوفمبر ٢٠١١م .

– الخطة الاستراتيجية بالمركز الوطني للإلكترونيات والاتصالات والضوئيات (وثيقة داخلية).

– التقرير السنوي لإدارة المشاريع بالمركز الوطني للإلكترونيات والاتصالات والضوئيات (وثيقة داخلية).

– مقال تقنية الإلكترونيات والاتصالات والضوئيات، مجلة العلوم والتقنية ، العدد ١٠٠ شوال ١٤٣٢هـ / أغسطس ٢٠١١م.

مدينة الملك عبدالعزيز للعلوم والتقنية KACST

شهادة استحقاق

المراعي Almarai

إن المجلس الأعلى لجائزة المراعي للإبداع العلمي وبعد إطلاعه على جميع الاعمال المرشحة
وعلى تقرير أمانة الجائزة وتوصيات المحكمين
قرر منح

جائزة الوحدة البحثية في مجال الاتصالات وتقنية المعلومات ١٤٣٣ هـ / ٢٠١٢ م
وان المجلس إذ يمنح هذه الشهادة
للمركز الوطني للإلكترونيات والإتصالات والضوئيات
بمدينة الملك عبدالعزيز للعلوم والتقنية
ليرجوا الله أن يمد منسوبي المركز بالعون لمواصلة الجهود العلمية المتميزة

رئيس مدينة الملك عبد العزيز للعلوم والتقنية
د. محمد بن إبراهيم السويل



جائزة المراعي للإبداع العلمي

رئيس مجلس إدارة شركة المراعي
الأمير سلطان بن محمد بن سعود الكبير

■ شهادة استحقاق من شركة المراعي.

الـنُّظُم الرقمية

م/ياسر بن محمد صديق



يكثر الحديث في عصرنا الحاضر عن التقنيات الرقميّة (Digital technologies) التي دخلت في كلِّ نواحي حياتنا، فكم شهدنا من تقنيات قد عرفناها واستخدمناها، ولكن أعيد تسويقها بعد تحويرها، لتصبح ضمن التقنيات الرقمية التي هي أصغر حجمًا وأفضل أداءً وأقل ثمنًا مقارنة بما كان قبلها، ومن أمثلة ذلك: التلفاز والمذياع ومسجِّلات الصوت. لقد شاعت التقنيات الرقميّة وتلقّاها الناس بالقبول وفضّلوها على ما ليس رقميًا، ما دفع الإنسان إلى عدِّها حلًّا لمشكلاته التي واجهها مع التقنيات القديمة، بل أن هناك سعيًا حثيثًا من روّاد التقنية ومُصَنِّعيها لإضفاء الصبغة الرقميّة على التقنيات الوليدة والموجودة.

يتناول هذا المقال تقنيات النُّظُم الرقميّة بدءًا من التعريف بالجيل السابق من التقنيات والنُّظُم، وتحديد مواطن الضعف والقصور فيها، وكيف استطاعت النُّظُم الرقمية التفوق عليها.

الإشارات والـنُّظُم

يعتمد المهندسون في تصميم النُّظُم الإلكترونيّة القديمة والحديثة على تطوير وظائفها كي تتمكّن من معالجة الإشارات الداخلة إليها، لتخرج إشارات أخرى بمواصفات متغيرة وفقًا للوظيفة التي من أجلها صمم ذلك النظام، لذلك ينبغي التعرّف أكثر إلى الإشارات، ومن ثم نستطيع فهم النُّظُم. فالإشارة هي علاقة بين مُتغيّرين أو أكثر، وجميعها متغيّرات مستقلّة ــ لا تتأثر بهذه العلاقة بل تؤثر فيها ـ إلا متغيرًا واحدًا فقط يكون تابعًا لهذه المتغيّرات المستقلّة، ولا يمكننا تحديد قيمته أو حالته إلا بعد تحديد قيمة أو حالة المتغيّرات المستقلّة، ومن أمثلة الإشارات في حياتنا اليوميّة درجات الحرارة المسجّلة خلال يوم كامل، فتلك علاقة بين متغيّرين، حيث نجد أن المتغيّر المستقلّ هو الزمن، و يمكن قياسه بالسّاعات، بينما المتغيّر التابع هو درجة الحرارة، ويمكن قياسها بالدّرجات المئويّة، ويوضح الشكل (١) مثالًا على إشارة درجات الحرارة خلال ساعات اليوم، فلو سُئِل أحدٌ عن درجة الحرارة سؤالًا مطلقًا دون تحديد الزمن المطلوب فلا يمكن الجواب عن ذلك السؤال حتى يحدّد السائل السّاعة التي يعنيها، فلو كان السائل يقصد درجة الحرارة التي سُجّلت عند الساعة الثامنة صباحًا فيمكنك الرجوع إلى الإشارة التي في الشكل (١) لتعرف أنّ درجة الحرارة في تلك الساعة كانت ثلاثًا وعشرين درجة مئوية، و بهذا يتّضح لنا أنّ درجة الحرارة هي إشارة لا يمكن تحديد قيمتها إلا إذا حدّدنا قيمة الزمن أوّلًا، فقيمة درجة الحرارة متغيّرة تابعة للزمن، بينما الزمن متغيّر مستقلّ يمكن تحديده دون الرجوع إلى درجة الحرارة.

الجدير بالذكر أنّ معظم النُّظُم الإلكترونية المستخدمة في حياتنا تعالج الإشارات الداخلة إليها لتولِّد إشارات أخرى يُستفاد منها، وقد تخضع هذه الإشارات الخارجة هي الأخرى إلى معالجات عدّة من خلال سلسلة من النُّظُم حتى تكتمل الوظيفة النهائيّة التي طوّر الإنسان من أجلها هذه النُّظُم التي يكمِّل بعضها بعضًا كما يحدث في أنظمة الاتصالات والبث التلفزيوني والإذاعي، حيث إنّ هذه النُّظُم تعالج عدّة أنواع من الإشارات لتصل - في نهاية الأمر - إلى إشارات يمكن إدراكها بأسماعنا وأبصارنا التي هي أيضًا أنظمة معقّدة تحوّل هذه الإشارات إلى إشارات عصبيّة تنتهي إلى العقل البشريّ الذي يعالجها للوصول إلى نتيجة نهائيّة يستفيد منها الإنسان.

من أمثلة النُّظُم الإلكترونية المشهورة -منذ زمن بعيد في حياتنا- هي مسجّل أشرطة الصوت أو أشرطة الكاسيت الذي يحوّل إشارات الصوت إلى إشارات كهربائيّة متّصلة الزمن، ثم يخزّنها في الشّريط ثم يستعيدها متى طُلب منه ذلك، فيحوّل الإشارات التي يستلمها من الشريط إلى إشارات أخرى تنتهي بإشارات صوتيّة ندركها بأسماعنا، ومثال آخر هو المذياع (الراديو) الذي يستقبل إشارات الراديو الكهرومغناطيسية التي تبثّها محطّات الإذاعة لاسلكيًّا في الجو فيحوّلها إلى إشارات كهربائيّة أيضًا يعالجها عبر دوائر



■ شكل (١) درجات الحرارة المسجلة خلال ساعات اليوم.

إلكترونيّة ما ينتج عنه استخراج إشارة الكلام المتضمَّنة في الإشارة المستلَمة، ثم تحويلها إلى إشارة صوتيّة ندركها بأسماعنا، فنعلم ما يقوله المذيع في استوديوهات الإذاعة.

يتعامل هذان النظامان مع الإشارات الصوتيّة التي يتكوّن منها الكلام البشريّ، ويمكن تمثيل هذه الإشارة بيانيًّا من خلال قياس مقدار شدّة صوت الإنسان، وبما أن النُّظُم الإلكترونيّة لا تحسن التعامل إلا مع الإشارات الكهربائيّة فإنها لن تستطيع التعامل مع الإشارات الصوتيّة قبل أن تتحوّل إلى إشارات كهربائيّة، وعليه تُسوّغ هذه الحقيقة ضرورة وجود الميكروفون في أيّ نظام إلكتروني يعالج الأصوات: كالهاتف والمسجل، حيث إنّه هو النظام المسؤول عن تحويل إشارات الصوت إلى إشارات كهرباء يمكن للنُّظُم أن تتعامل معها كهربائيًّا، ويبيّن الشكل (٢) إشارة كهربائيّة أنتجها الميكروفون نتيجة لدخول إشارة صوتيّة صدرت عن متكلّم حينما كان ينطق بكلمة (لِسَان)، ويقاس الزمن بوحدة الملّي ثانية، وهي جزء من ألف جزء من الثانية، بينما تقاس مخرجات الميكروفون بالفولت، وهو وحدة قياس فرق جهد الإشارات الكهربائية عمومًا، ويوضح الشكل (٢) إشارة كلمة لسان، وكذلك تفاصيل الإشارة التي نتجت عن نطق حرف اللام وتتبعها إشارة الكسرة ليُكوِّنا معًا اللام المكسورة التي تبدأ بها كلمة لِسان.

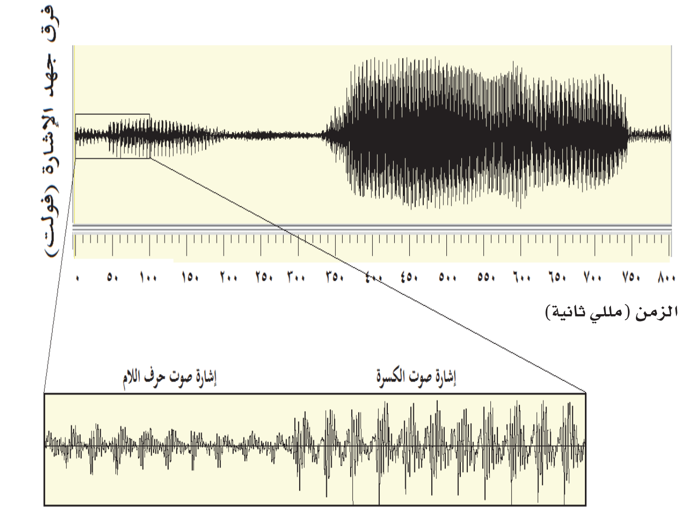
دوافع ظهور النظم الرقمية

على الرغم من استفادة الإنسان - لسنين عدّة- من كثير من النظم السابقة لظهور الأنظمة الرقمية، إلا أنّه واجه بعض العقبات بسبب طبيعة تلك النُّظُم التي عجزت عن تلبية مطالبه المتزايدة، وعن استيعاب التعقيدات التي تصاحب تلك المطالب، ومن أمثلة ذلك:

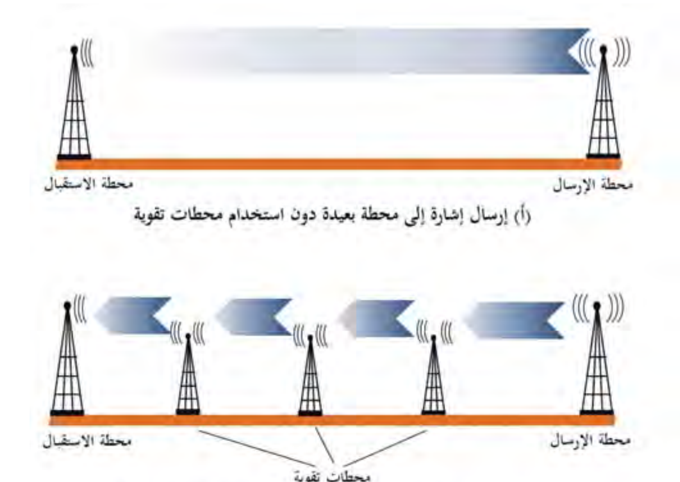
١- تعرّض الإشارة للتشويش وللتداخل قبل وصولها إلى النظام الذي يستقبلها ما يؤدّي حتمًا إلى تغيّر قيمتها، فلا يملك النظام في هذه الحالة سوى أن يعالجها كما وصلته، ليخرج لنا الإشارة التي قد لا نرضى عن جودتها و نقائها إذا كان التداخل والتشويش شديدين، و إن كان هذا الخطأ قد لا يكون مؤثرًا كثيرًا في بعض التطبيقات، إلا أنه أمر مقلق جدًا في تطبيقات أخرى.

٢- ضعف الإشارة لطول المسافة بين المرسِل والمستقبِل، فلا يستطيع نظام الاستقبال تقويتها وتصفيتها إن كانت المسافات بعيدة جدًّا، وعندئذ يمكن استخدام أنظمة لتقوية الإشارة على مراحل متتابعة بين موقعَي المُرسِل والمستقبل، بحيث تعمل تلك المقوّيات على استقبال الإشارة قبل أن تدخل في حالة الضعف الشديد، ثم تُصفِّيها وتعيد بثّها تارة أخرى بعد تقويتها حتى تصل إلى المستقبِل الأخير في حالة يمكن معها الاستفادة من تلك الإشارة، ومن أمثلة ذلك يوضح الشكل (٣) كيف استخدمت شدّة اللّون لتوضيح شدّة الإشارة، حيث يوضح في الشكل (٣-أ) أنّ الإشارة بعد أن قطعت مسافة طويلة وصلت إلى محطّة الاستقبال وهي في حالة ضعف شديد يتعذّر معها استفادة المستقبِل منها، بينما يوضح الشكل (٣ - ب) أنّ استخدام محطات التقوية ساعد على استدراك الإشارة قبل خفوتها، حيث تم تجديد قوّتها بإعادة بثّها من جديد إلى المحطة التالية، وهكذا تستمر السلسلة حتى تصل إلى محطة الاستقبال بقوّة مناسبة يمكن التعامل معها. إنّ خضوع الإشارة لعمليّة التقوية لا يمكن أن يعيدها أبدًا لقيمتها الأصليّة، و لكن إلى قيمة أخرى قد تكون قريبة من القيمة الأصليّة، و بهذا فإنّ كلّ نظام تقوية سوف يكون مصدرًا لإضافة الأخطاء إلى مقدار الإشارة، إما بالزيادة أو النقصان، ومع طول المسافات وكثرة المقوّيات تزداد الأخطاء في قراءة مقدار الإشارة وتتراكم حتى تصل إلى تدهور واضح في جودتها و نقائها.

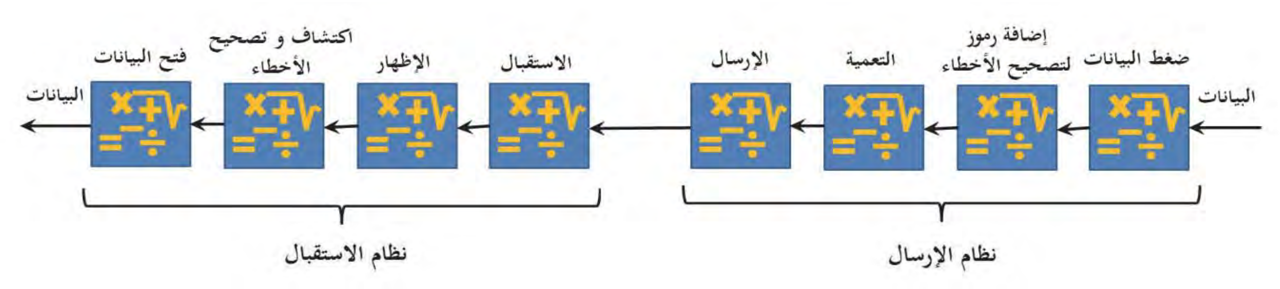
٣- التشفير: حيث لم تلبي الأنظمة القديمة تعمية (تشفير) الإشارات لغرض حماية البيانات التي تحتويها من التجسّس، كما يحدث في بعض نُظُم الاتصالات الآمنة، حيث يُعَمَّى محتوى الإشارات قبل إرسالها ثم يتم إظهار المحتوى عند وصول الإشارة إلى نظام الاستقبال، بأن تُزال هذه التعمية بطرق وخطوات متّفق عليها بين نظامي الإرسال والاستقبال، حيث إن عمليات التعمية اليوم قد تطوّرت عمّا كانت عليه في الماضي، بحيث واكبت الطلب المتزايد عليها نظراً لأهميتها وضرورة وجودها في كثير من النُّظُم الحديثة،



▪ شكل(٢) إشارة كهربائية تمثل قراءة الميكروفون للصوت الناتج عن نطق كلمة لسان.



▪ شكل(٣): تأثير محطات التقوية على زيادة المسافة بين محطة الإرسال والاستقبال.



■ شكل (٤): خضوع بيانات الإشارة لبعض العمليات الحسابية قبل الإرسال وأخرى عكسية بعد الاستقبال.

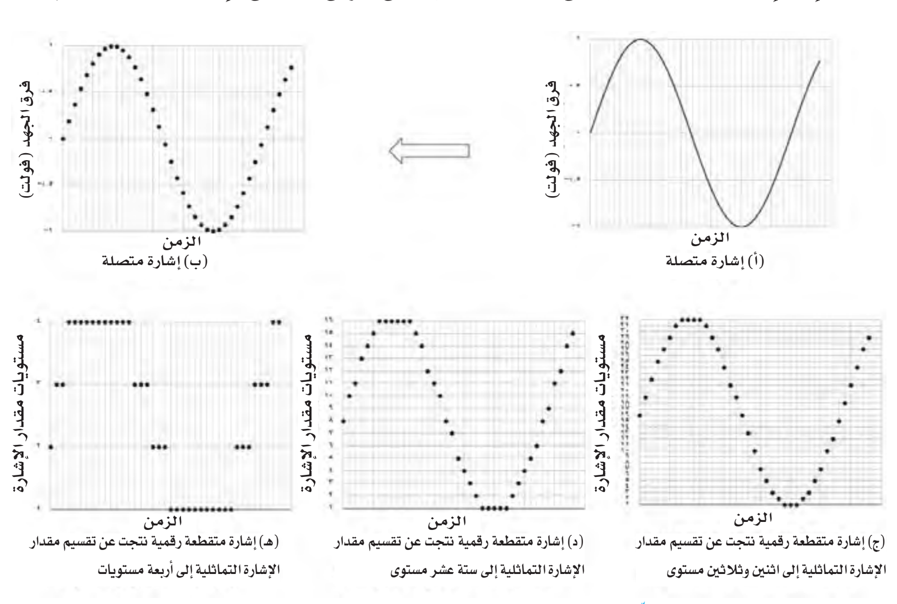
وأصبح من الصعب جدًا كشف البيانات المُعَمّاة. إنّ نُظُم التعمية تؤدي وظيفتها من خلال إخضاع الإشارة لعمليات حسابيّة قبل إرسالها، ثم تخضع الإشارة المرسَلة لعمليات حسابيّة عكسيّة لدى استقبالها تكون نتيجتها إزالة التعمية عن الإشارة، وإظهار الإشارات الأصلية، ويوضح الشكل (٤) أمثلة لبعض العمليات الحسابيّة التي قد تخضع لها بيانات الإشارة قبل الإرسال، والعمليات الحسابيّة العكسيّة بعد الاستقبال، إضافة إلى ذلك، فإن الإشارة قد تخضع لعمليّات حسابيّة إضافيّة بهدف اكتشاف أيّ أخطاء طارئة على مقدارها وربما تصحيحها، وهناك أيضًا عمليات أخرى تهدف إلى تقليص زمن الإشارة أثناء إرسالها (زمن الإرسال)، ومن ثَمَّ زيادة سرعة الاتصال وتقليص حجم التخزين تمامًا، كما يحدث في حالة الملفات في الحاسب وهو ما نسمّيه «ضغط البيانات أو ضغط الملفات» شكل (٤). وهناك كثير من العمليّات غير تلك التي ذُكِرَت نحتاج إلى أن نطبّقها على الإشارات للحصول على نتائج و خصائص أفضل، وتلك العمليات الحسابيّة متقدّمة ومعقّدة ويجب أن تطبّق على أرقام محدّدة، وفي لحظات يمكن إحصاؤها حتى يمكننا إعادتها لأصلها بصورة صحيحة ودقيقة.

الإشارات ذات المقدار الرقمي

يتضح مما سبق أنّ الإشارات بشكلها الذي كانت عليه في الماضي تقف عاجزة أمام تلبية كثير من متطلبات الإنسان الحديثة نظرًا لما أسلفناه من تأثرها الشديد بالتشويش، وصعوبة إرسالها لمسافات بعيدة، وصعوبة إخضاعها لكثير من العمليّات الحسابيّة بغرض تعميتها أو تصحيحها أو ضغطها، و غير ذلك من مواطن الضعف والقصور فيها، ولذلك فلا بدّ من تغيير طبيعتها لجعلها أكثر تقبّلًا لتلك العمليات والتحدّيات، وذلك من خلال خطوتين هما:

١- عدّ لحظات الإشارة الزمنيّة خلال مدّة معيّنة، وذلك بأخذ عيّنات منها خلال لحظات معدودات في تلك المدّة، ونكتفي بها مع تجاهل كلّ القيم الواقعة خلال اللحظات التي لم نجمع خلالها العيّنات كما في المثال الموضّح في الشكل (٥)، وهكذا فإنّ الإشارة ستفقد طبيعتها المتّصلة، ويمكن تسميتها حينئذ بالإشارة المتقطّعة، وبما أنّها تتكوّن من لحظات يمكن عدّها، فإنّ الإشارات المتقطّعة يمكن أن تدخل في كثير من التطبيقات الجديدة التي عجزت عنها الإشارات المتّصلة، مثل تناوب مستخدمي الهاتف على استخدام خط واحد مشترك.

٢- تقسيم مقدار الإشارة لمستويات محدّدة ومعدودة، بحيث يُعطى كلُّ مستوى منها رقمًا صحيحًا (الأرقام الصحيحة هي ١، ٢، ٣، ٤، ...) بحيث تقع كلّ قيمة من قيَم الإشارة ضمن أحد تلك المستويات، وبدلًا من استخدام القيمة الأصلية للإشارة في لحظة من اللحظات يستخدم رقم المستوى الذي تنتمي إليه، وحينئذ سيصبح لدينا إشارة ذات مستويات مرقّمة، ولذلك اصطُلح على تسمية هذا النوع من الإشارات «إشارة رقمية». شكل (٥). حيث يلاحظ أنّ الإشارة في الشكل (٥-أ) قد أُخذت منها عيّنات لتصبح إشارة متقطّعة، شكل (٥-ب)، وبعد ذلك يمكن تكوين عدد من الإشارات المتقطّعة الرقميّة



■ شكل (٥) إحصائية إشارات متقطّعة رقميّة نتجت عن تقسيم مقدار الإشارة المتقطعة التماثلية إلى مستويات معدودة.

إذا قسَّمنا قيم المتغيّر التابع إلى مستويات معدودات، كما يلاحظ في الشكل (٥-ج) و (٥-د) و (٥-هـ).

إنّ تقسيم مقدار الإشارة إلى مستويات وترقيم القيم حسب مستوياتها هو في حقيقة الأمر تغيير لمقدار الإشارة إمّا بالزيادة أو بالنقص، وهذا التغيير ما هو إلا خطأ نضيفه عمدًا إلى الإشارة، ومن الضروري معرفة كيفيّة التحكّم بهذا الخطأ الحاصل ومدى تأثيره في معلومات الإشارة، وبالنظر إلى شكل (٥) يلاحظ أنّ مقدار الإشارة المتقطّعة الرقميّة (ج) قد قُسِّم إلى اثنين وثلاثين مستوىً، ويقابل ذلك ستة عشر مستوىً في مقدار الإشارة (د) وأربعة مستويات في مقدار الإشارة (هـ)، ويلاحظ أنّ أكثر الإشارات شبهًا بالإشارة الأصليّة هي الإشارة (ج) التي هي الإشارة ذات أكبر عدد من المستويات، ثم تليها الإشارة (د) ثم أخيرًا الإشارة (هـ) التي هي أقلّ الإشارات الرقميّة شبهًا بالإشارة (ب). ويعود السبب في ذلك إلى أنّها صاحبة أقلّ عدد من المستويات، ومن ثَمَّ يمكن استنتاج أنّه كلما زاد عدد مستويات التقسيم قلّ الخطأ الذي يطرأ على الإشارة، ومن ثَمَّ ستكون الإشارة أكثر شبهًا بالإشارة الأصليّة التي اشتُقّت منها، والعكس صحيح، فكلما قلّ عدد المستويات سيقلّ الشبه بينها وبين الإشارة الأصليّة.

عندما تتم معالجة الإشارة داخل النُّظُم الرقميّة فإنها تكون متقطّعة الزمن رقميّة المقدار، بحيث يمكن التعامل معها على أنّها أرقام منفصلة عن بعضها بعضًا يعالجها النظام الرقميّ من خلال عمليّات حسابيّة تعطي النتائج المطلوبة بكلّ دقة وكفاءة، فالنُّظُم الرقميّة ما هي إلا حاسبات متخصّصة في تطبيق معيّن تتفاوت في قدراتها وتعقيداتها، وبما أنّ الإشارة أصبحت مجموعة من الأرقام، فإنّها يمكن أن تفتح آفاقًا جديدة من التطبيقات، وتلبي المزيد من المتطلبات الحديثة، وتتفوّق على الإشارات التماثلية في كثير من النواحي. فمثلًا لا تتأثر الإشارات الرقميّة بكثرة محطات التقوية، حيث يمكن لكلّ نظام تقوية أن يعيد الإشارة للقيمة نفسها التي أرسلت بها إذا استدركها مبكّرًا قبل أن يعتريها ضعف شديد، وبذلك ترجع لحالتها الأولى بدقة ولا يؤدّي طول المسافة إلى تراكم الأخطاء وتشويش الإشارة واضمحلالها، وكذلك يمكن للإشارات الرقميّة أن تدخل في عمليات التعمية، واكتشاف الأخطاء وتصحيحها، وضغط البيانات وتخزينها وإعادة إنتاجها، وغير ذلك من العمليّات الهندسية الكثيرة والمعقّدة.

النُّظم الرقميّة في حياتنا

تُعدُّ النُّظُم الرقميّة حاضرة وخادمة وفعَّالة في جميع جوانب حياتنا اليوميّة، فنشاهد التلفاز الرقميّ الذي يعرض قنواتٍ من نظام الاستقبال الرقميّ الذي يستقبل إشارات من قمر اصطناعي رقميّ، وكذلك حين نُجري مكالمة بالهاتف الجوال فإنّنا نوظّف هذا النظام الرقميّ لإرسال كلامنا بصورة إشارات رقميّة لأبراج الاتصالات الرقميّة إلى حيث الطرف الآخر من المكالمة، ومثله المذياع، فإنّه وإن لم يكن رقميًّا خالصًا بعد، إلّا أن له أزرار تحكّم رقميّة وواجهة استخدام رقميّة، فبات بالإمكان التنقّل بين الإذاعات، وحفظ تردّدات الموجات باستخدام الدوائر الرقميّة التي في المذياع، وليس المذياع وحده الذي أصبح ذا واجهة استخدام رقميّة، بل أكثر أجهزة المنزل كالغسّالة والثلّاجة والفرن، و بتصوّر أشمل فالنُّظُم الرقميّة ما هي إلّا نظم إلكترونيّة تؤدّي وظيفتها عن طريق معالجة الأرقام، وبهذا التصوّر يمكن اختزال أيّ نظام رقميّ في كونه حاسبًا مصغّرًا متخصّصًا في أداء وظيفته التي صُمِّم لأجلها، فحينئذ سنكتشف أنّ النُّظُم الرقميّة حاضرة معنا في السيّارة، حيث إنّ أنظمة التحكّم في المحرّك والوقود والحرارة و غيرها ما هي إلا نُظُم رقميّة لا نراها مباشرة، لكنّها ضرورية كي تؤدّي السيارة وظيفتها، ومثلها نُظُم التحكّم في الطائرة، فلا يؤدّي الطيّار مهمّة دون استخدام العديد من النُّظُم الرقميّة كنظم الملاحة الجوية والرادارات، ونظم الاتصالات، سواء في الطائرات المدنيّة أو الحربيّة، وإذا انتقلنا إلى المستشفيات فما ينفكّ الأطباء والمرضون محتاجين في غرف العمليات والعناية المركّزة إلى النُّظُم الحسّاسة الدقيقة الرقميّة التي تُستخدم لقياس ضغط الدم ونبض القلب والوظائف الحيويّة في جسم الإنسان كافة، وعليه لا يمكن حصر الأمثلة للنُّظُم الرقميّة، فقد باتت عاملًا مهمًا في كل جوانب حياتنا.

الخلاصة

اتضح من خلال ما تناولناه آنفًا أنّ النُّظُم التي استخدمها الإنسان في الماضي لعشرات السنين- ولا تزال تستخدم في مجالات عدّة وتطبيقات متنوّعة- قد ظهر فيها بعض جوانب الضعف والقصور في الأداء مع تزايد متطلّبات الإنسان وكثرة تعقيدات التطبيقات الحديثة، وعليه لجأ مهندسو النُّظُم الإلكترونيّة إلى تقطيع زمن الإشارة من خلال أخذ عيّنات منها، ورقّموا مقدار العيّنات المأخوذة من خلال تقسيم المقدار إلى مستويات معدودات ثم ترقيمها، لينتج عن ذلك الإشارات الرقميّة التي يمكن معالجتها بالنُّظُم الرقميّة الحاسوبيّة، فكانت بفضل الله سببًا لفتح آفاق رحبة لكثير من التطبيقات، ولحل كثير من المشكلات و التحدّيات التي يواجهها الإنسان.

المراجع

-Alan Oppenheim, Alan Willsky and Hamid Nawab, “Signals and Systems”, 2nd edtion Prentice Hall.

-Lathi, B. P., Modern Digital and Analog Communication Systems, 4th Ed., 2002, McGraw-Hill, New York

-Steven W. Smith, “The Scientist and Engineer›s Guide toDigital Signal Processing”, online : “http://www.dspguide.com”



شبكة الهاتف العامّة

م. ياسر بن محمد صديق



لم يكُنْ باستطاعة النّاس في الماضي التّواصلُ مع بعضهم بعضًا من مسافات بعيدة بالسّهولة التي نعيشها نحن اليومَ عبر وسائل الاتّصالات الحديثة، غير أنّ مُحاولات الإنسان المستمرّة لاختراع حلول لمشكلاته تمخّضت عن تطوّر وسائل الاتّصال بشتّى أشكالها، منها الهاتف الذي يَنْقل محادثاتنا الصّوتية عبرَ شبكة الهاتف العامّة إلى شتّى أرجاء الأرض؛ حتّى أصبحَ الهاتفُ من أهمّ الوسائل التي لا يستغني عنها المرءُ في حياته.

من المُحاوَلات الجادَّة التي كانت تقصد إلى صنع آلة تُمَكّن الإنسانَ من التحدّث بصوته عبر مسافات بعيدة تلك المحاولات والتّجارِب التي كان يجريها **ألكسندر جراهام بل** في الولايات المُتّحدَة الأمريكيّة، التي انتهت بتجربته النّاجحة في عام ١٢٩٣هـ الموافق ١٨٧٦م؛ إذ نجح في التّواصل صَوْتيًّا مَعَ مُساعِده عبر آلة صنعها، وبهذا الحدث كانت بداية دخول الهاتف إلى حياة النّاس، وبداية صناعة تقنيات الاتّصالات الصّوتية وتطوّرها، وسُرْعان ما بدأ النّاس يُقْبلون على شراء أجهزة الهاتف، ويوضّح الشكل (١-أ) الهاتفَ المُستخدَم في أثناء التّجارب، في حين يوضّح الشكل (١-ب) الهاتفَ المُستخدَم بعد إعلان الاختراع.



(١-أ) شكل الهاتف المُستخدَم في أثناء التجارب. (١-ب) شكل الهاتف المُستخدَم بعد إعلان الاختراع.

■ شكل (١) جهاز الهاتف حين اختراعه.

تتلخّص وظيفة جهاز الهاتف سواء بشكله البدائيّ أم بشكله الحديث - الذي نعرفه اليوم- في أنّه جهازٌ يربط المستخدمين بشبكة الهاتف، ويحوّل الموجات الصّوتيّة التي يُصْدرُها المُتكلِّم في أثناء كلامه إلى إشارات كهربائيّة، تُنْقَل عبر الأسلاك إلى الطّرف الآخر من المكالمة؛ إذ يحوّل جهازُ هاتفٍ آخرَ هناك تلك الإشارات الكهربائيّة إلى موجات صوتيّة يسمعها الطّرف الآخر كما هو مُوضَّح في شكل (٢)؛ فالجزء الذي يُحوِّل الصَّوت إلى كهرباء يُسمَّى الميكروفون، وهو الذي يُوضَعُ قريبًا من فم المتكلِّم، أمّا الجزء الذي يُحوّل الكهرباء إلى صوت يُسمَّى السَّمّاعة، وهي التي تُوضَع مُلاصقة للأذن؛ فوجود السّماعة والميكروفون في جهاز الهاتف يمكّننا من الكلام والسّماع عبر الهاتف في الوقت نفسِه، و تُنْقَل الإشارات الكهربائيّة عبر سلك الهاتف الذي يتكوَّن في داخله من سلكَيْن وذلك لاستكمال

■ شكل (٢) تحويلُ الهاتفِ الصّوتَ إلى كهرباء والعكس.

الدائرة الكهربائية وسريـان التيار عبر السلكين بين طرفي المكالمة.

جديـر بالذّكـر أنّ النّاس الذيـن استخدموا الهاتـفَ في أيّامـه الأولى، شـكل (١) لم يكـنْ باستطاعتهـم السّمـاعُ والـكلامُ في الوقت نفسه كمـا نستطيع اليوم، بل كان علـى المتكلِّم أن يضع جهـازَ الهاتـف أمـام فمـه إن أراد أن يتكلّم، ثم يضعـه في أذنه ليسمع ردّ الطَّـرَف الآخر؛ بمعنى أنّ الهاتفَ في ذلك الزمن لم يكن مُزَوّدًا بسمّاعة ومايكروفـون، بـل كان هناك جهـازٌ واحدٌ فقط، يؤدّي الوظيفتين معًا.

تطـوّر شبكـة الهـاتـف

بـدأت شبكـةُ الهاتـف في أيّامهـا الأولى بصـورة يسيرة وبدائيّـة؛ إذ كان كلّ خطّ هاتفيّ لا يربـط سـوى هاتفين اثنـين فقط؛ فمثـلًا إن أراد شخصـان أن يتواصلا عـن طريق الهاتف؛ فـكان يلزمهما شـراءُ جهازَيْ هـاتـفٍ يُرْبَطَان بسلك يمتدّ من موقـع المُستخدِم الأولِ إلى مَوْقِع المُستخـدِم الثّـاني، وبذلـك يمكنهمـا التّحدث فيمـا بينهما مباشَـرة وحصريًّا؛ بمعنـى أنّ أيًّا منهمـا لـن يستطيـع استخدام هاتفـه ليتحدّث إلى شخصـ غير ذلك الشخص الذي يرتبط به هاتفـه؛ ولهذا فقـد كان ضروريًّا أن يصبحَ لدى كلّ شخصـ عدّة هواتـف في بيتـه أو مقرّ عمله بعـدد الأشخاص الذيـن يريد التّحـدّث إليهم، ويوضّـح شـكل (٣) مثـالًا لشبكةِ هاتـفٍ تضمّ عشرةَ مُستخدِمين؛ إذ يظهر بوضوح كيف أنّ كلّ مستخـدِم من هؤلاء لـن يتمكّنَ مـن التّواصـل معهـم جميعًـا، فمثلًا المُستخدِمـان (ج) و(ي) يمكنهمـا التّحدّث فيمـا بينهما فقـط؛ لوجـود سلـك يربطهما، في حـين يبـدو المُستخـدِم (ب) أفضل حالًا؛ إذ بإمكانه التحدّثُ إلى المُستخدِمـين (هـ) و(ز) و(ح)، ولكنْ يَلْزَمـه شراءُ ثلاثة هواتفَ، يَستخدم كلَّ واحد منها للاتّصال بأحد أولئك الثّلاثة.

● **المَقْسَم الهاتفيّ**

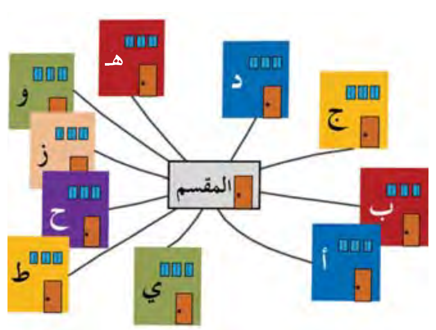
لم تكن طريقة تلـك الخدمة الهاتفيّة مُكْلفَة على المُستخدِمين فحسب؛ بسبب اقتنائهم لأكثرَ من هاتف في البيت الواحد، بل إنّ كمّيّة الأسلاك المُمْتدّة بـين المباني خَلَقَتْ فوضى في المُدُن خلال العامَـيْن الأوّلَـيْن من استخدام الهـاتِف، فكان الحلّ الأنسبُ هو أن تُنَظَّمَ شبكة الهاتف بطريقة تكُـون أكثرَ فعاليّةً وراحةً؛ بحيث تُوصَّل الهواتف جميعهـا في المنطقـة بمكتـب مركـزيّ يُحَـوّل المكالمات بين الهواتف حَسب ما يريده المشتركون مقابـل مبلـغ اشـتراك. ويُسَمَّـى هـذا المكتـب (Switching office) ويُطْلَـق عليـه في البلـدان العربيـة عدّة أسماء، منهـا: المَقْسَـم، والبَدَّالة، والمُحَـوِّل، والسِّنـترال، ويوضّح شـكل (٤) كيفيّةَ استخدام المَقْسَم في تنظيم شبكة الهاتف موازنة مع شكل (٣)، ذات الأسلاك العديدة. كان تحويل المكالمـات في المَقْسَـم حينئذٍ يتمّ يدويًـا بوساطة مُوظَّـف يَستقبـل المكالمات مـن المشتركين؛ بحيث يلزم المُتَّصل أن يُكلِّمَ مُوظَّف المَقْسَم بخطٍّ مُباشَر بينهمـا، ويحدّد له مَـن هو المُشـترك الآخرُ الذي يريـد مكالمته، فيقوم الموظَّف بتوصيل طرف سلك المشـترك المتّصـل بطرف سلك المشـترك الآخر؛ لتكتَمِلَ الدّائـرة الكهربائيّة بينهمـا؛ فتتمّ المُكالمة مُباشَـرة، وهكـذا صـار بإمـكان أيِّ مُشـترك أن يتّصلَ بأيِّ مشتركٍ آخرَ في المَقْسَم الهاتفيّ نفسه.

● **المَقْسَم الهاتفيّ الآليّ**

أصبـح المَقْسَـم الهاتفـيّ جُـزْءًا أساسيًّا في أيّ شبكـة هاتـف في العالم منـذ ذلك الحين إلى يومنـا هذا، وقد تطـوّرت المَقاسِم عـبر السنين؛ فبعـد أن كان مُوظّـف المَقْسم يستقبـل المكالمات ويوجّهها يدويًا أصبـح توجيه المكالمات في المَقْسَم يتـمّ آليًـا دون تدخـل أيّ موظّـف. وقـد بـدأت المحاولات العلميّة لتطويـر مَقْسَم آليّ بعد حوالَيْ عشر سنين من بداية استخـدام المَقْسَم اليدويّ، وبـدأت المَقاسِم الآليّـة تزاحم المَقاسِـمَ اليدويّة رويـدًا رويدًا؛ حتّـى أصبح موظّـف المَقْسَم جزءًا مـن الماضـي، وأضْحَـتْ شبـكاتُ الهاتـف توجّه المُكالَمـات حسـب أرقـام المشتركين. فعنـد تأمّل أرقام الهواتف ستجـد أنّ فيها أرقامًا تميّز البلد الـذي ينتمـي إليه ذلـك الرقـم ومدينتـه وربّما الحي، وهذا هـو المبدأ الذي يعتمده المَقْسَم الآليّ لتحويل مكالماتنا، ويعدّ إدخال رقم الهاتف بمقام مُخاطَبة المَقْسَم؛ لإخبـاره بوجهة المُكالَمَة؛ لتترك له مَهمّـة توصيلـك بالمُشترك الآخـر الذي تريد مكالمته، فاللّحظات اليسـيرة التي تنتظرها على الخـطّ بعد إدخـال الرقـم وقبـل أن تسمع نغمة استلام مكالمتك تكون المَقاسِم مشغولة بتوصيلك بالطّـرَف الآخرِ، وإكمال الدائـرة بينكما، وحالمًا تكتمل الدائرة ستسمـع النغمة المتقطّعة المألوفة،



■ شكل (٣) شبكة الهاتف مربوطة بأسلاك مُوَصَّلة مباشرة بين الهواتف المختلفة.



■ شكل (٤) شبكة الهاتف مربوطة بأسلاك هاتفية عن طريق المقسم.

التـي تفيـد بنجـاح الاتّصـال بالطّـرَف الآخر، أو بانشغال الخطّ لديه بمكالمة أخرى.

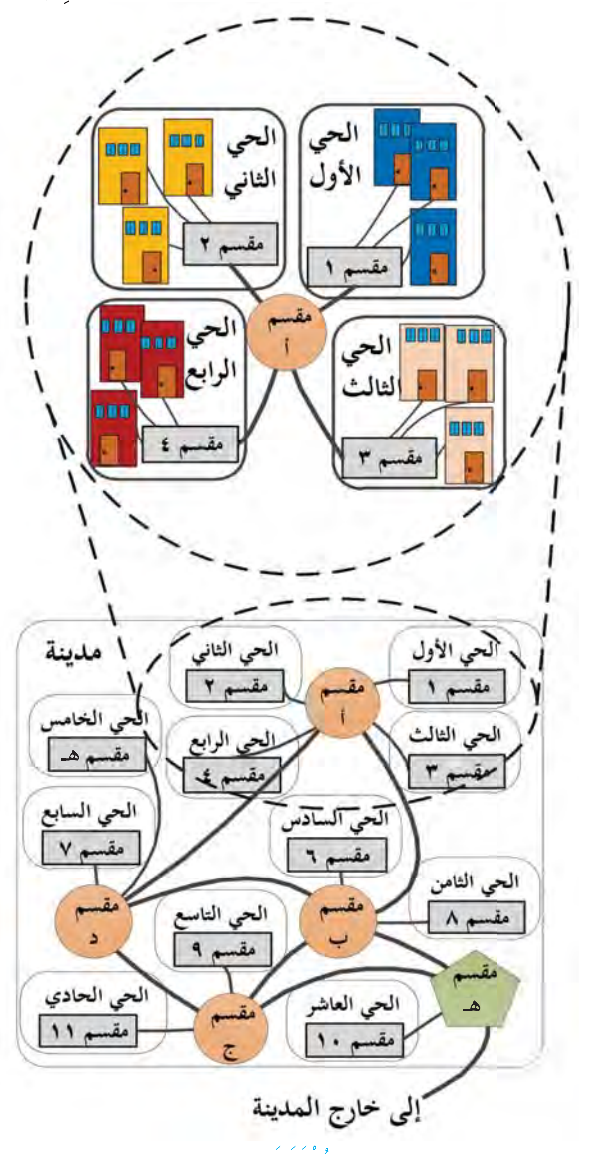
● **تمرير المكالمات عبر المَقاسم الهاتفيّة**

منـذ الأيّام الأولى لاستخدام المَقْسَم نشأت الحاجـة إلى توصيل المكالمات بـين هاتفَـيْن تفصلهما مسافة بعيـدة جدًّا؛ بحيث لا يجمعهما مَقْسَمٌ واحدٌ، بل يرتبط كلّ منهما بمَقْسَم مختلف عن الآخـر كأن يكونـان في مدينتَـيْن متّجاورتَيْن مثـلًا، فكان من الضّـروريّ أن تُربَط المَقاسم مع بعضها بعضًا؛ ليصبـح المَقْسَم مسؤولًا عن ثلاث وظائف أساسيّة، هي:

١- ربط بعض مُشتركي ذلك المقسم ببعض.

٢- ربـط مشتركـيّ المَقْسَـم بالمقاسـم الأخـرى البعيدة؛ ما سيمكّنهم مـن التّواصل مع مشتركيّ تلك المَقاسم.

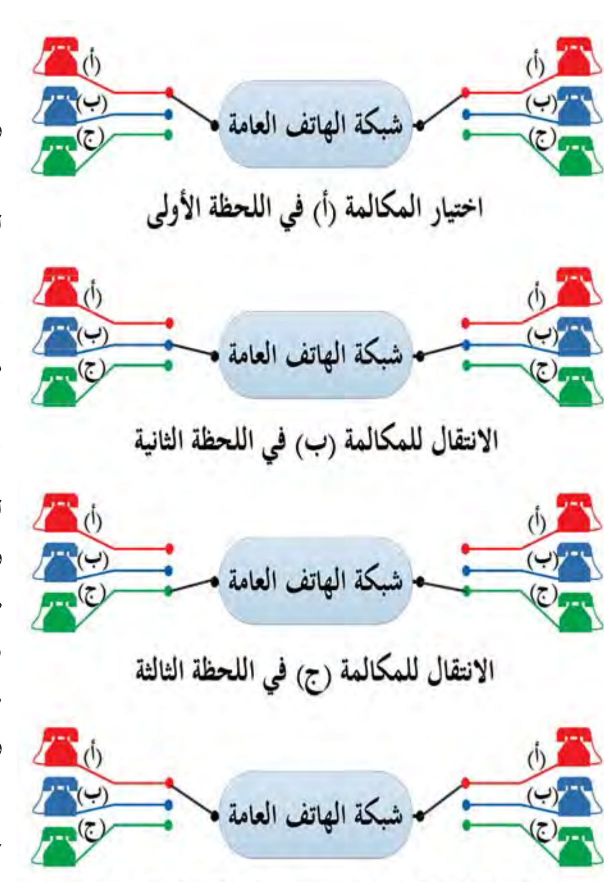
٣- تمريـر المَقْسَـم المكالمـات التـي تصـل إليـه من مَقاسمَ بعيـدة، لكنّها غـيرُ مُوَجَّهَة لمشتركي المَقْسَـم، بل إلى مَقْسَم آخـرَ؛ بحيث يكون حلقة وصـل بينهما. تجـدر الإشارة هنـا إلى أنّ توزيع المَقاسـم في شبـكات الهاتـف يختلف مـن شبكة لأخـرى باختـلاف البلـدان وكثافـة المشتركـين واتّصالاتهـم، ويبيّن الشكل (٥) مثـالًا مُفْتَرَضًا لشبكـة هاتـف عامّة تربـط سكّان مدينـة ما مع بعضهـم بعضًـا، ومـع مدينـة أخـرى مُجـاورة؛ ولكـي نفهـم طريقة تحويـل المكالمـات من خلال المَقاسم الهاتفيّة سنستخدم ذلك المثال؛ فلو أراد أحَـدُ سـكّان الحـيّ الأوّل من تلك المدينة إجـراءَ مُكالَمة هاتفيّة؛ فإنّه سيدخل الرّقـم الهاتفيّ للمشترك المطلـوب، وستعمـل المَقاسـم بناءً على ذلـك الرقـم؛ إذ إنّـه يحتوي التعليمـات جميعهـا التـي تحتـاج إليهـا المقاسـم لأداء مهامّها، فإن كان الرقم لمشترك في الحيّ نفسه فـإنّ المقسـم الداخلي هـو المَقْسَم (١) لذلك الحـيّ سيوجّه المكالَمة، وينطبـق الشّـيء نفسه علـى بقيّة الأحيـاء ومقاسمهـا. لكـنْ لو كان الرّقـم لمشـترك في الحـيّ الثـانيّ مُرتبـط بالمَقْسَم (٢) فـإنّ المكالمة ستبـــدأ من المَقْسَـــم (١) الذي يحوّلُها إلى المَقْسَم (أ) الذي بدوره سيحوّلهـا إلى المَقْسَم (٢) فتنتهي إلى هاتـف المُشـترك المطلوب، أمّا إذا كان الرّقـم لمشـترك في الحـيّ العاشـر المرتبـط بالمَقْسَـم (١٠) فعندئـذ ستمـرّر المكالمة من خلال عدد أكبرَ مـن المقاسم نظرًا لعدم وجود مَقْسَم يربط المَقْسَمَيْن (١) و(١٠) مباشَـرة، فسيقوم المَقْسَم (١) بتوجيـه المكالمـة للمَقْسَم (أ) فيمرّرهـا للمَقسَـم (ب) الـذي يمرّرهـا للمَقْسَـم (هـ)؛ لكـي يمرّرهـا أخيـرًا للمَقْسَـم (١٠)؛ إذ يربطهـا بالمشترك المطلوب. ويلاحَـظ مـن خلال ذلـك المثـال كذلـك أنّ أيّ مكالمـة موجّهة إلى خارج المدينة لا بدّ من أن تمرّ خلال المَقْسَم (هـ)، ولا يعني هذا بالضرورة أنّ في شبكات المُدن مقسمًا واحـدًا لتوجيه المكالمات خـارج المدينة، فيمكـن أن يكون هنـاك أكثرُ من مَقْسَمٍ يربطها بالخارج.



■ شكل (٥) مثال لشبكة هاتف مُفْتَرَضَة في مدينة ما.

تقنيات المَقاسم والرّبط بينها

من الطبيعيّ إجراءُ أكثرَ من مكالمة هاتفيّة داخل الحيّ الواحد في الوقت نفسه، ويستطيع المَقْسَم المحلّيّ أن يتعامـل مع هـذه الحالات وخدمة كلّ المشتركين معًـا؛ فالمكالمات الموجَّهة لمشتركين في الحيّ نفسه تمرَّر مباشَرة، وليس على المَقْسَم المحلّيّ سوى ربط أطراف المكالمات بأسـلاك خاصّة لـكلّ مكالمة؛ إذ يتـاح العدد الـكافي من الأسـلاك داخـل المَقْسَـم المحلّيّ؛ فيخصِّـص سلْـكًا حصْريًّا لكلّ مشـترك، أمّا في حـال المكالمات الموجَّهـة إلى خـارج المَقْسَم المحلّـيّ؛ فالأمـر يختلـف قليـلًا؛ إذ إنّ المَقْسَم المحلّـيّ عادة يملِـكُ سِلْـكًا واحـدًا فقط يمرّر مـن خلالـه المكالمـات إلى خـارج المَقْسَـم، ويستقبل من خلالـه المكالمات كذلك، فيصعب حينهـا التّعامُـلُ مع أكثر من مكالَمـة في الوقت نفسـه، ولهـذا تطبَّق تقنيـة الاختيـار الزمني (Time multiplexing) شكل (٦)، التي تمكِّن المَقْسَـم من خدمة أكثر مـن مشترك واحد في الوقـت نفسه من خـلال تخصيص مدّة زمنيّة قصـيرة لكلّ مشترك يتاح له استخدام السّلك الخارجيّ للمَقْسَم، وعند انتهاء تلك المُدّة يُمْنَح السّلـكُ لمستخدم آخـرَ للمُدّة نفسهـا، وهكذا يستمرّ التّناوب بين المستخدمين حتّى يعود الدور إلى المستخدم الأوّل من جديد، وتستمرّ الدورة بسرعـة شديـدة لا تؤثّـر في جـودة المكالمات، ولا يشعـر معهـا المتكلّمـون بتقطّـع المكالمـة. لكـنْ هناك حدٌّ معيّنٌ للمكالمـات التي يمرّرهـا المَقْسَـم في الوقت نفسه لا يستطيع بعدَهـا أن يَقْبَـلَ أيّ مكالمات جديدة؛ لأنّ مدة تلك الدّورة



■ شكل (٦) التّناوب بين المكالمات بتقنية الاختيار الزمنيّ.

ستَطُـول حتّى يتاح السّلـك مرّة أخرى لمشترك مـا، وهذه المـدّة الطّويلة كافية لتقطّعَ الصّوت وتَدَهْـوِرَ جودة المكالمة، ولذلك يلجأ المَقْسَم إلى الاعتذار عن عدم قبول مكالمات جديدة إن كان ذلك سيؤثّر في تمرير المكالمات الجارية حاليًّا، وعندئذ ستسمع رسالة اعتذار تفيد بتعثّر مرور مكالمتك والمحاولة لاحقًا.

شبكـــــات الهاتــــف

تُعَـدّ شبـكاتُ الهاتِـف إحـدى أشهـر الشبكات السلكيّة، وأكثرها أهميّةً في العالم؛ لكـون بعضِ أجــزاء الشّبكـة مرتبطٌ ببعض عن طريـق أسلاك ممتدّة تحـت الأرض أو فوقهـا؛ إذ إنّ المَقاسِم المحليّة داخل الأحياء مربوطة ببيوت المشتركين بأسلاك نحاسيّة، وكذلـك يربـط المَقْسَـم المحلـي بالمقاسـم الأخرى البعيدة بالأسـلاك ذات السّرعات العاليـة؛ حتّـى تتمكّـنَ مـن استيعـاب مكالمـات أكـثَرَ وأسرعَ، فتَسْتَخْدِم الأسلاك النّحاسيّة والألياف الضوئيّة لهذا الغرض.

وليـس بالضّــرورة أنّ كلّ أجزاء شبكة الهاتف مربوطة مـع بعضهـا بعضًـا بوساطة الأسـلاك، فقــد تُستخـدَم أحيانـاً روابـط لاسلكيّـــة؛ لربـط المناطــق البعيـدة، وحيثمـا كان تمديد الأسلاك صعبًـا ومُكْلِفًـا، ومـن أمثلـة ذلـك تمريـرُ المكالمـات عـن طريق الأقمـار الاصطناعية وأبـراج المايكرويـف، وننبّـه القـارئَ الكـريم هنـا إلى عـدم الخلــط بـين أبـراج المايكرويف المُستخدَمَـة ضمن شبكـة الهاتــف وأبــــراج شبكــة الجَوّال.

الإنترنت عبر شبكة الهاتف العامّة

بعد التطوّرات العديدة التي طرأت على تقنيات شبكة الهاتف العامّة عبر عشرات السّنين وانتشارها الواسع، أصبحت مـن أهمّ المكوِّنات التي لا يَستغني عنهـا سـكان أيّ مدينـة مـن مـدن العـالم؛ حتّـى وَصَلَـتْ إلى معظم البيوت والمكاتـب، وبدأ الاهتمام باستغلالهـا لأغراض غـير المكالمـات الصوتيّـة كالإنترنـت مثلًا؛ نظرًا لأنّ النّجاح في توظيف شبكة الهاتـف لخدمة أغراض أخرى سيُغْني عن إنشاء شبـكات جديـدة في المـدن وتمديدها. وبعـد مضيّ قـرن من اختراع الهاتِف لأوّل مـرّة أصبح بالإمكان نقلُ بيانـات الإنترنت عبر شبكة الهاتف، وهو الأمر الـذي مَهَّد لتطوّر خدمـات الإنترنت وشبكة الهاتف معًا خلال السنين التي تلت ذلك النجاح.



■ برج مايكرويف لربط شبكة الهاتف.

إنّ صعوبة نقل بيانات الإنترنت عبر شبكة الهاتف تكمـن في أنّ شبكـة الهاتـف بمُكوّناتهـا وتمديداتهـا جميعها، وبمبدأ عملها مهيـأة أصلًا؛ لنقل الإشارات الكهربائية إلى الكلام، دون الأخذ بالحسبان أنّ تلك الشّبكة سوف تتعامل مع نوع آخرَ من الإشارات؛ ولذلك كان مـن الضـروريّ سدّ الفجـوة بين تقنيـة الهاتف وتقنيـة الإنترنـت، فكان ذلـك دافعًا لاخـتراع جهاز يُحَوِّل بيانـات الإنترنت الرّقمية التـي تناسب طبيعة الحاسـب إلى إشارات تناسب طبيعـة شبكة الهاتف، وقـد سُمِّـيَ ذلـك الجهـازُ مـودم الاتّصـال الهاتفي (Dial-up modem). ويُعَدّ جهازُ المودم بصورة عامّة أيَّ جهـازٍ إلكـتروني يقـوم بمُهمّـة تضمـين البيانات المـراد إرسالُها ضمن مَوْجَة يسهـل معها إرسال تلك البيانات، كمـا يستخرج المودم البيانـات المضمَّنة في المَوْجَـة المُستَقْبَلة؛ ولهذا فـإنّ مودم الاتّصال الهاتفيّ ما هو إلا مودم صُمِّمَ خصّيصًا؛ لتضمين البيانات في موجات تستطيـع شبكة الهاتـف أن تميّزها، وترحّبُ بنقلها إلى حيـث يحوّل مودم آخـرُ في الطّرَف الآخر من الشّبكة الإشـارة مرّة أخرى إلى إشارات يستطيع الحاسب أن يميّزها، وفي هـذه الخدمة تنتقل بيانات الإنترنـت عـبر شبكـة الهاتف كمـا لو كانـت مكالمة صوتيّة، وهـذا يفسّر عدم تمكّننا من إجراء مكالمات صوتيّـة أو استقبالهـا أثناء تصفّحنـا الإنترنت عبر مودم الاتّصـال الهاتفي، ويوضّـح الشكل (٧) مودم



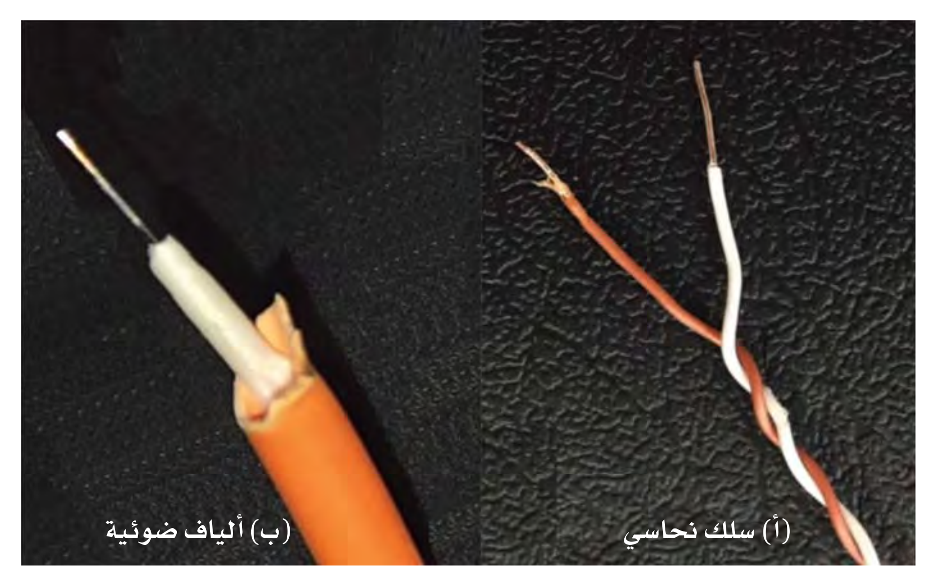
■ شكل (٧) أحـد أنـواع مـودم الاتّصـال الهاتفـيّ المُلْحَق بالحاسب.

اتّصال هاتفيّ مُجَهَّز للعمل مُرْفَقًا بالحاسب، ويَظْهَر فيه منفذُ سلك الهاتف الذي يتواصل المودم- من خلاله- مع شبكة الهاتف العامّة.

بعد أن وَجَدَ مودم الاتّصال الهاتفي طريقه إلى بيوت المشتركين ومكاتبهم، وأصبح وجوده ضمن أجزاء الحاسب أمرًا ضروريًا، تزايدت الحاجة إلى سرعات عالية للاتّصال بالانترنت. غير أنّ قدرات مودم الاتّصال الهاتفي لم تمكِّنه من تلبية تلك السرعات؛ نظرًا لكونه يتعامل مع إشارات ضمن تردّدات أصوات المكالمات، وهذه التردّدات غيرُ قادرة على حمل البيانات بسرعات عالية من تلك التي يتيحها مودم الاتّصال الهاتفيّ، ويعود سبب ذلك القصور إلى أنّ مَقْسَم شبكة الهاتف بطبيعته سيتجاهل أيّ إشارة ذات تردّد خارج نطاق تردّدات أصوات المكالمات، وبهذا أصبح من الأفضل حلّ المشكلة في المقسم الذي هو جزء من شبكة الهاتف بدلًا من حلّها في بيوت المشتركين، فكانت الخطوة نحو زيادة سرعات الإنترنت باستخدام جيل جديد من المقاسم الهاتفية تَقْبَل تردّدات أعلى من تلك المَقاسم القديمة، فأصبح باستطاعة المشتركين الحصولُ على سرعاتٍ أعلى عن طريق الخدمة التي باتت مشهورة بين الناس باسم خطوط المشتركين الرّقمية (Digital Subscriber Lines -DSL).

عندما يشترك أحد سكّان الحيّ في خدمة خطوط المشتركين الرّقميّة؛ فإنّ شركة الهاتف ستنقل طرف سلك ذلك المشترك من المَقْسَم القديم إلى المقسم الجديد دون أن يدري بذلك، ولكن يبقى عليه أن يستخدم مودمًا خاصًّا بهذه الخدمة يكون في بيته أو مكتبه. يُسَمَّى هذا المودم مودم خطوط المشتركين الرّقمية (أو ما يُسَمّيه الناس مودمَ DSL)، ويرسل بيانات الإنترنت ويستقبلها عبر إشارات رقميّة معزولة تمامًا عن إشارات المكالمات الصّوتية للهاتف، لا كما كان يفعل مودم الاتّصال الهاتفيّ؛ لذلك تجد أنّ مودم خطوط المشتركين الرّقمية يُمَكّن المشتركين من إجراء مكالماتهم الهاتفية في حين أنهم - في الوقت نفسه - يتمتّعون بتصفّح الإنترنت.

قد يحدث أحيانًا عدم تمكّن شركات الهاتف من تزويد بعض المشتركين بخدمة خطوط المشتركين الرقميّة في بعض الأحياء، ويعود السّبب في ذلك إلى أنّ المقاسم المحليّة في تلك الأحياء لم تُرَقَّ بَعْدُ لاستقبال الخطوط الرقمية، وقد يحدث أحيانًا أن تتفاوت السّرعات المتاحة للمشتركين في الحيّ الواحد؛ لبعدهم وقربهم من المقسم المحلي؛ فكلّما كانت المسافة بين المشترك و المقسم المحليّ قريبة أمكنه الحصولُ على سرعات أعلى مقارنة مع المشتركين المقيمين بعيدًا عن المَقْسَم.



■ شكل (٨) نوعين من الأسلاك المستخدمة في شبكة الهاتف.

استمرّ التطوّر وزيادة السّرعات في مَقاسم خطوط المشتركين الرقميّة منذ طرحها للمشتركين عامًا بعد عام، ولكنّ الأسلاكَ النُّحاسيَّة المُستخدَمة في شبكة الهاتف بسبب خصائصها الفيزيائيّة لها قدرةٌ محدودة على نقل البيانات؛ إذ لا تستطيع تجاوز سرعات معيَّنة في نقل البيانات حتّى وإن كان المَقْسَم قادرًا على إتاحة تلك السّرعات؛ ولهذا أصبحت الأسْلاك النّحاسيّة عَقَبَةً في طريق تطوّر الإنترنت عبر شبكة الهاتف، فكان من الضّروريّ استخدامُ موادَّ بديلة من النّحاس، فجاء الدَّوْر لترقية الأسلاك التي تربط المشتركين بالمقسم المحلي؛ إذ اُسْتُخْدِمَتِ الأليافُ الضّوئيّة إلى جانب الأسلاك النحاسيّة؛ ما فتح المجال أمام سُرعات عالية لنقل بيانات الإنترنت عبر الألياف الضوئيّة، فيما بَقِيَتِ الأسلاك النّحاسيّة، شكل (٨)، لنقل المكالمات والبيانات بسرعات أقلّ.

الخلاصة

منذ اختراع الهاتف ومعه شبكة الهاتف العامّة وعبر ما يزيد على القرن وثلث القرن من الزمن تطّورت شبكة الهاتف العامّة؛ لتصبح شبكةً مُتعدِّدة الاستخدامات بعد أن بدأت شبكةً بدائيّة مَحدودة الانتشار والقدرات، وقد شمل ذلك التطوّر شتّى جوانب الشّبكة؛ فحيث بدأت محدودةً للمكالمات الصّوتية فحسب، أصبح استخدامُها يشمل الإنترنت بشتّى جوانبه، وقد تطوّرت مكوِّنات الشبكة؛ لتشمل الألياف الضوئيّة، والأقمار الاصطناعيّة، وروابط المايكرويف، ولا تزال شبكات الهاتف تشهد تزايدًا في الانتشار والخدمات مما يبشّر بمستقبلٍ أفضل لهذه الوسيلة التي باتت من ضروريّات الحياة.

المراجع

-Andrew S. Tanenbaum, Computer Networks, 4th edition, Prentice Hall PTR, 2003.
-Cisco Systems Inc. Internetworking Technologies Handbook, 3rd edition, Cisco Press, 2000.
-William Stallings, Data and Computer Communications, 6th edition, Prentice Hall, Inc., 2000.
http://www.museumphones.com
http://www.antiquetelephonehistory.com
www.made-in-china.com
http://www.bidorbuy.co.za

الدكتور أسد علي عبيدي

من رواد علم الإلكترونيات في العالم

عالمنا لهذا العدد أحد أبرز علماء الإلكترونيات، حيث تلقّى تعليمه في المملكة المتحدة البريطانية والولايات المتحدة الأمريكية واللتان تعدان من أهم دول التقنية، كما أثمرت جهوده البارزة في وضع لمساته لمدرسة العلوم والهندسة التابعة لجامعة لاهور للعلوم الإدارية مما جعلها تنافس أبرز جامعات التقنية في العالم كمعهدي ماساتشوستس (MIT)، وكاليفورنيا للتكنولوجيا (Caltech)، وقد ساهم ذلك في ظهور جيل من العلماء والمهندسين للمساهمة في تحويل المشهد الاقتصادي والتقني في باكستان. كما يعد عبيدي من الباحثين الذين ساهموا في تطوير تقنية «RF-CMOS» التي لعبت دوراً أساساً في ثورة الاتصالات اللاسلكية في تسعينيات القرن الماضي، كما نال العديد من العضويات العلمية وفاز بعدة جوائز.

الأسم: أسد علي عبيدي

الجنسيه: باكستاني، أمريكي.

مكان وتاريخ الميلاد: لاهور، باكستان، ١٢يوليو، عام ١٩٥٦م.

التعليم

- البكالوريوس: في مجال الهندسة الكهربائية من كلية امبريال في لندن، عام ١٩٧٦م.
- الماجستير: من جامعة كاليفورنيا، بيركلي، عام ١٩٧٨م.
- الدكتوراه: من جامعة كاليفورنيا، بيركلي، عام ١٩٨١م.

العمل الأكاديمي

تدرج الدكتور عبيدي في العمل الأكاديمي الذي كان حافلاً ومتنوعاً كما يلي:

- عضو الفريق الفني للمختبرات المتقدمة (Bell Laboratories) في مدينة موراي هيل بولاية نيو جيرسي بأمريكا، من عام ١٩٨١ - ١٩٨٤م.
- سكرتير مؤتمر دوائر أشباه الموصلات الإلكترونية، منظمة (IEEE)، من عام ١٩٨٤ – ١٩٩٠م.
- أستاذ الهندسة الكهربائية والإلكترونية في جامعة كاليفورنيا، لوس أنجلوس، بأمريكا، من عام ١٩٨٥م إلى الآن .
- باحث زائر في مختبرات (HP- Hewlett Packard)، عام ١٩٨٩م.
- الرئيس العام لندوة (VLSI Circuits) للدوائر الإلكترونية المتكاملة،عام ١٩٩٢م.
- سكرتير مجلس(IEEE) لدوائر أشباه الموصلات الإلكترونية، عام ١٩٩٠-١٩٩١م.
- محرر في مجلة(IEEE) لدوائر أشباه الموصلات الإلكترونية، عام ١٩٩٢- ١٩٩٥م.
- أول عميد لجامعة لاهور للعلوم الإدارية - مدرسة العلوم و الهندسة، لاهور، باكستان حيث ساعد في تشكيل الأيام الأولى لهذه المؤسسة الجديدة مما وضعها على قائمة أبرز الجامعات التقنية في العالم.

الجوائز وشهادات التقدير

نال الدكتور العبيدي العديد من الجوائز تقديراً لجهوده وتميزه العلمي ومن أهم تلك الجوائز :

- جائزة (TRW) للطرق المبتكرة في التدريس، عام ١٩٨٨م.
- جائزة أفضل ورقة عمل في المؤتمر الأوروبي ٢١ لدوائر أشباه الموصلات الإلكترونية، عام ١٩٩٦م.
- جائزة (Donald G. Fink Prize) ، منظمة (IEEE)، عام ١٩٩٧م.
- جائزة ورقة العمل التكنولوجية باسم (Jack Raper Outstanding Technology Directions)، في مؤتمر (ISSCC)، عام ١٩٩٧م.
- جائزة مسابقة التصميم للدوائر الإلكترونية في المؤتمر العالمي (DAC)، عام ١٩٩٨م.
- وسام الألفية الثالثة، منظمة (IEEE)، عام ٢٠٠٠م.
- اختير ضمن أفضل عشرة كتّاب، مؤتمر (ISSCC)، عام ٢٠٠٢م.
- جائزة (Donald O. Pederson)، منظمة (IEEE)، عام ٢٠٠٧م.
- جائزة (UCLA HSSEAS Lockheed Martin) للتميز في التدريس، من جامعة كاليفورنيا، لوس أنجلوس، الولايات المتحدة، عام ٢٠٠٨م.

العضويات

حصل الدكتور العبيدي على عدة عضويات علمية منها :

- عضو مميز في(IEEE) – منظمة مهندسي الكهرباء والإلكترونيات، من عام ١٩٩٦م إلى الآن.
- عضو في الأكاديمية الوطنية للهندسة، عام ٢٠٠٧م.
- عضو في أكاديمية العلوم للعالم الثالث، عام ٢٠٠٩م. التي أسسها الدكتور الباكستاني محمد عبد السلام الحاصل على جائزة نوبل في الفيزياء، عام ١٩٧٩م.

الكتب

ألف الدكتورعبيدي عدد من الكتب العلمية في مجال التخصص.

المراجع

- http://www.ee.ucla.edu/people/faculty/faculty-directory/asad-abidi
- http://lums.edu.pk/faculty/abidi
- http://propakistani.pk/200902/04//scientist-profile-dr-asad-abidi/

الهواتف المحمولة الذكية

م/ أيمن صالح بدوي

تعاقبت وسائل الاتصال واحدة تلو الأخرى محدثة فوارق تقنية عظيمة لم يكن يتخيلها الإنسان، فحينما ظهر الهاتف الثابت بأول جيل له كان ذلك بمثابة الابتكار الخارق الذي أبهر العالم بكيفية إجراء محادثة صوتية بين شخص وآخر من حول العالم مما وفر الوقت واختصر المسافات وجعل العالم كقرية واحدة، بعدها ظهر نوع آخر من الهواتف سمِّي بالهاتف النقال (السيار) بشكله التقليدي القديم وبحجمه الكبير وهيبته التي كان يعطيها مالكه والذي مكن المستخدمين - بشكل خاص رجال الأعمال وكبار الشخصيات - من إجراء المكالمات من السيارة. تلا ذلك ظهور النوع الثالث من الهواتف (المحمول) من قبل شركة موتورولا والذي أضاف خدمة الشبكة اللاسلكية التي وضعت في كل مكان وأطلق عليها مزود الخدمة المحلي من خلال أبراج «محطات»الإرسال والاستقبال، حيث كان لكل برج سعة محدودة لعدد المكالمات المستقبلة والمرسلة، كما ميّز أجهزة تلك الجيل أنها أقل استهلاكا للطاقة إضافة لإرسال الرسائل النصية والصوتية والمكالمات الصوتية. وتوالت بعدها النماذج المتطورة من جهاز الهاتف المحمول إلى أن لقب بـ «الذكي» بمواصفات مبتكرة تواكب ظهور شبكة الجيل الثالث وبرزت فيه مميزات كثيرة كالاتصال القوي بالإنترنت وبسرعة عالية وإمكانية إجراء المكالمات المرئية والكاميرا المدمجة ذات الجودة العالية ونظام تحديد المواقع الجغرافية كما أنه احتوى على نظام تشغيل متطور جعلته أقرب ما يكون للحاسب الآلي المحمول .



حقق الهاتف المحمول الذكي رغبات كثيرة للمستهلك وغطى معظم احتياجاته اليومية، كما ساهمت أيضا جهات أخرى ولعبت دورا آخر تكاملا مع هذا الجيل بإضافة تطبيقات شبيهة بتطبيقات الحاسب الآلي(مثل البرامج)، وتطبيقات أخرى مختلفة للمواقع الإلكترونية للجهات الحكومية والتعليمية والترفيهية والتوعوية وغيرها. جاء كل ذلك مصاحبًا لتنافس الشركات المصنعة للأجهزة المحمولة وتعاونهم مع مطوري البرمجيات للهواتف المحمولة الذكية.

بمشاهدة التغيرات الجذرية بين الهاتف المحمول التقليدي والهاتف الذكي يتضح أن هناك عوامل رئيسة ميزت الهاتف الذكي كالحجم الأصغر والوزن الأخف وجودة الصوت العالية والشبكات القوية وذكائه بوجود (نظام في شريحة) الذي يعد بمثابة العقل المدبر للمحمول الذكي والمسؤول عن أضخم العمليات وأعقدها في الهاتف المحمول.

أمثلة من الأجهزة الذكية

تتميّز هذه الهواتف عن غيرها في وجود النظام في شريحة (SoC-System on Chip) الذي يوجد في جهاز آيفون المصمم من قبل شركة أبل، كذلك جهاز جالكسي المصمم من قِبل شركة سامسونج وجهاز إتش تي سي١ (HTC1) من قِبل شركة (HTC). وتعد هذه الأجهزة جميعها متشابهة في معظم المواصفات ولكن يأتي الاختلاف في تطوير بعض الأجزاء لتتواءم مع تطور التقنية وطلبات المستخدم. ملبين في ذلك طلبات المستهلك كالبطارية الأمثل، والمعالجات الرسومية الأقوى، وكاميرا بدقة عالية، ونظام سريع ومرن، ونظام الخصوصية والأمان، وغيرها من المزايا.

مزايا الأجهزة الذكية

تختلف مزايا الجهاز المحمول الذكي من جهاز لآخر، لذا يصعب على المستخدم اختيار ما يلائمه من الأجهزة الذكية لاختلاف مواصفاتها

وتباينها في بعض المزايا عن الأخرى، ومن الممكن أن يتميز جهاز عن الآخر و قد تؤدي هذه الميزة لثقل وزنه مثلًا أو كبر شاشته. ويمكن إبراز أهم المزايا التي توفرت في الجهاز المحمول الذكي فيما يأتي:

- **الشاشة**

بدأت تظهر مجددا شاشات كبيرة الأحجام و التي جعلت حجم الجهاز يبدوا أكبر من سابقه، حيث كان المستهلك يبحث عن أصغر الأجهزة ولا يعتني كثيرا لأمر الشاشة ولكن سرعان ما عادت رغبة المستخدم للأجهزة الأكبر لاحتوائها على شاشات كبيرة باختلاف أنواعها المختلفة مثل (Retina display)، (Super AMOLED)، وغيرها، التي جاءت لتحاكي تطلعات المستخدم في مشاهدة مقاطع مرئية بجودة أعلى وحجم شاشة أكبر. كما دعمت شاشة المحمول الذكي ألوانا عميقة ونوعيات أكثر مما كانت عليه في الهاتف التقليدي. وينبغي التنبـــــه أنه كلما زاد حجـــم الشاشـــة زاد احتياجها لاستهلاك البطارية.

- **نظام التشغيل**

كانت الأجهزة المحمولة القديمة عادة ما يسودها نظام تشغيل واحد لا يقوم إلا بمهام رئيسية، وعندما جاء نظام التشغيل في المحمول الذكي كان مخالفا لسابقه، فهو يقوم بمهام رئيسية وثانوية تلبي احتياجات المستخدم .

تختلف أنظمة التشغيل في الأجهزة المحمولة الذكية باختلاف خصوصية النظام، فهناك أنظمة تشغيل مغلقة المصدر- مثل نظام تشغيل «iOS»، شكل (١) الموجود في جهاز آيفون - تختلف طبيعتها عن أنظمـــة التشغيل مفتوحـــة المصدر مثل نظام تشغيل «Android» الموجود مثلا في جهاز (جالكسي، اتش تي سي، وغيرهم) والذي يمكن المستخدم من التعديل في نظام التشغيل، حيث يأتي الاختلاف في أنظمة التشغيل في قدرتها الأكبر على تنظيم عمل المكونات الداخلية وتحقيق استفادة أكثر.

- **تصميم الجهاز**

تسعى كل الشركات إلى تحسين المظهر الخارجي للأجهزة بشكل يجذب المشتري، وهنا تختلف وجهات النظر للمستهلك فمنهم من يفضل الشكل الانسيابي أو متحدد الأطراف، ومنهم من يفضل ألوانا دون أخرى كالأبيض والأسود والأزرق وغيره. إضافة للإطار المحيط بالجهاز، فمنها البلاستيكي ومنها المعدني والذي يعد مهما في تصميم أي جهاز.

- **وزن الجهاز**

كانت كفاءة الهاتف المحمول - سابقا - هي العامل الرئيس في الجهاز، أما الآن فبالرغم من تفوق الأداء وزيادة كفاءة الجهاز الذكي إلا أن وزنه أخف من الأجهزة التقليدية ذات المواصفات الأقل. وتعد خفة وزن الجهاز تحديا في تصميم الأجهزة الذكية حيث أنه من المتوقع أنه بتطور المواصفات والمزايا أن تزيد المكونات الإلكترونية، وهذا ما قد يزيد من وزن الجهاز مما يشكّل تحديا للأجهزة المصنعة.

- **التوصيلات والمنافذ**

تختلف التوصيلات والمنافذ من جهاز لآخر باختلاف التقنيات التي تسعى لتطبيقها الشركة، فيوجد مثلاً منفذ للطاقة وتبـــادل البيانات السلكية مثل (USBv2.0, MicroUSB)، وكـــذلك مدخل شريحة الجـــوال مثل: (Nano-SIM, MicroSIM). إضافة لشريحة الذاكرة هناك بعض الأجهزة التي قامت بوضع منفذ لشريحة خارجية للذاكرة مثل شريحة (SD, Micro SD) التي تمكن المستخدم من استخراج الذاكرة وتشغيلها من أي جهاز آخر. كان جهاز الهاتف المحمول لا يأتي إلا بذاكرة مدمجة صغيرة الحجم لا يمكن استخراجها من الهاتف المحمول وكانت منافذ توصيل الجهاز بمنفذ الطاقة لا تعمل إلا بتوصيلها بمقبس الكهرباء فقط.

- **الكاميرا**

لا تتحدد جودة الصورة بمقياس دقة وضوح الصورة «بكسل» فقط، وإنما هناك عوامل أخرى تتحكم في جودة الصورة كفتحة العدسة وعدد «البكسلات» وغيرها.

وصلت دقة وضوح الكاميرات الخلفية للأجهزة المحمولة ٢٠,٧ ميجابكسل بضوء فلاش مختلف التقنيات مثل فلاش (LED) ثنائي اللـــون أبيض أصفر، أو فلاش (LED) أحادي، حيث أن لكل منهم مزايا مختلفة تميزه عن الآخر.

كما ضمّت الأجهزة المحمولة الذكية كاميرتين - أمامية وخلفية - تمكّن المستخدم من استخدامها حسب احتياجه ليس كالأجهزة المحمولة التقليدية التي لم تضم أية كاميرات.

- **البطارية**

تعد سعة البطارية ليست العامل الأساس في عمر البطارية كما يتوقع المستخدم، بل هناك عوامل أخرى تؤثر على استهلاك البطارية كالمعالج الرباعي أوالثماني النواة حيث يستهلك ثماني النواة طاقة أكبر، وكذلك تؤثر دقة الشاشة وحجمها على استهلاك البطارية.

- **تقنية الاتصال قريبة المدى**

وفرت تقنية الاتصال قريبة المدى (Near Field Communication-NFC) لأجهزة الهواتف المحمولة الذكية نقل البيانات لاسلكيا بطريقة آمنة، كما وفرت الجهد والوقت. ومن أهم تطبيقاتها هي ربط الهاتف بملحقاته. تختلف هذه التقنية عن تقنية الاتصال اللاسلكي (Bluetooth) بمدى أصغر للإرسال والإستقبال وكذلك حجم البيانات المرسلة والمستقبلة.



شكل (١) نظام تشغيل «iOS».

● **خاصية الأمان للتعرف على بصمات الأصابع**

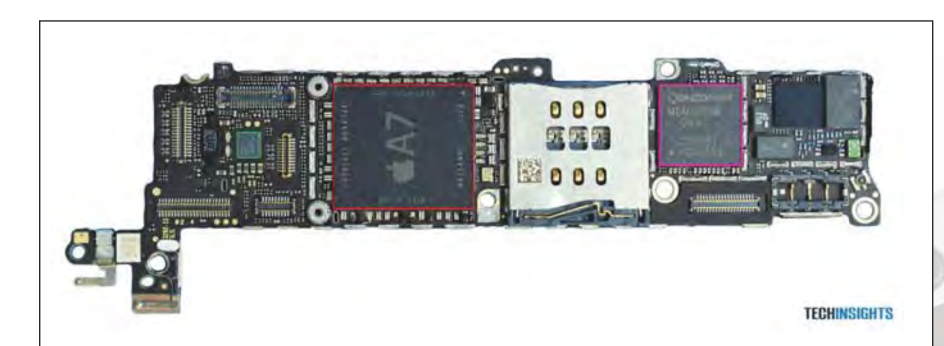
تعد هذه الخاصية تقنية حديثة مبتكرة بدأ تطبيقها للاستخدام الآمن للجهاز كالقيام بعمليات الدفع الآمنة وعدم السماح لغير مالك الجهاز بالعبث عن طريق مستشعر البصمات. وهذا يعكس ما ذكر من احتياجات المستخدم واختلاف المواصفات من شركة لأخرى التي تسعى لتحاكي رغبات المستخدم بما يوائم تصاميها أيضا.

● **دعم شبكة الجيل الرابع**

جاء دعم شبكة الجيل الرابع (Long Term Evolution-LTE) تبعــا لشبكات الهواتف الحديثة التي وفرتها شركات الاتصالات لتوفر سرعة اتصال بالانترنت أكبر من سابقتها بعشرة أضعاف، حيث دعمت فيها هذه الخدمة الأجهزة الحديثة وبالتالي قد يختلف سعر الجهاز الذي يضم هذه الخدمة عن ما إذا كانت هذه الخاصية غير مدعومة.

● **تقنية التصنيع المستخدمة**

يعتمد تصنيع «النظام في شريحة» والذي يضم المكونات الرئيسية في أي نظام مثل (وحدة المعالجة المركزية، وحدة معالجة الرسوميات، USB، وغيرها) بشكل رئيس على دقة التصنيع المستخدمة والتي تؤثر أيضا بشكل كبير على حجم الشريحة. تستخدم وحدة النانومتر في تصنيع هذه الشرائح ووصلت حديثا إلى ٢٨ نانومتر استخدمت في أجهزة تصنيع حديثة. توضح الأشكال(٢، ٣) التالية بعض التصاميم الموجودة على وجهي الشريحة أو اللوحة الأم للهاتف الذكي من الأمام والخلف.



القطع الإلكترونية	الشركة المصنعة
المعالج الرئيسي (نظام في شريحة) –شركة آبل	هاينكس
حساس الحركة للجهاز– شركة (ان اكس بي)	آبل
مودم المحمول لشبكات الجيل الرابع – شركة كوالكوم	برودكوم

■ شكل(٢): المكونات الداخلية للوحة الأم لأحد الهواتف الذكية (من الأمام).

ذاكرة مدمجة	هاينكس
إدارة الطاقة	آبل
واي فاي + بلوتوث	برودكوم
المتحكم في الصوت	آبل

TECHINSIGHTS

■ شكل(٣): المكونات الداخلية للوحة الأم لأحد الهواتف الذكية (من الخلف).

النظام في شريحة

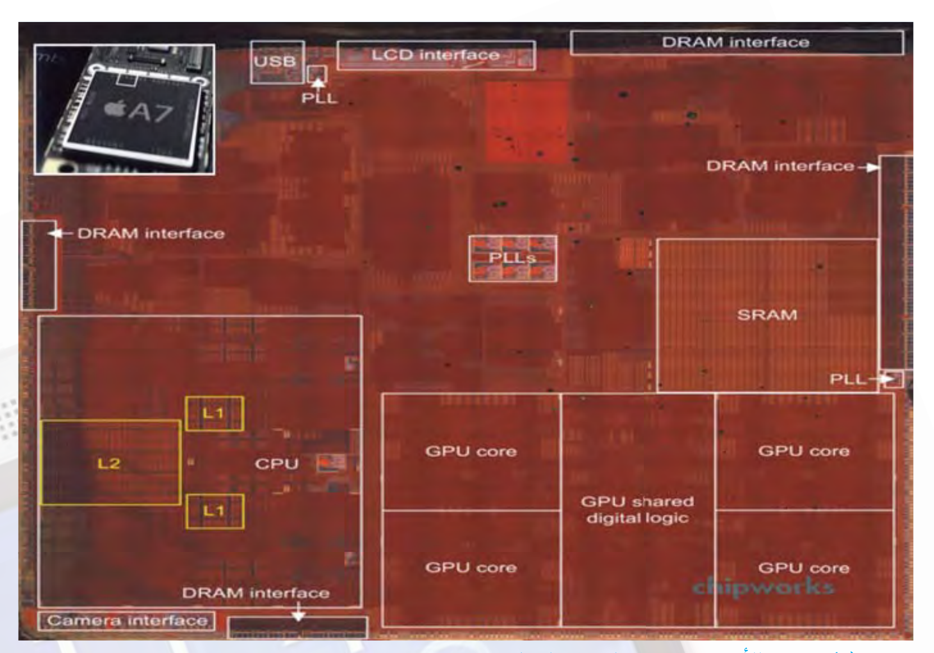
يعد النظام في شريحة مكونا رئيسا في معظم الهواتف المحمولة الذكية سعيا للتقريب بينه وبين أجهزة الحاسب الآلي، فهو بمثابة السر في كفاءة الهاتف المحمول الذكي و المعالج الرئيسي للتحكم في الجهاز. وعادة ما يكون تصميم هذا النظام لجهاز ما مشابها في معظم الأجزاء الرئيسية ويكون التشابه كبيرا خاصة إذا ما كان الجهاز من نفس الجيل، أو إذا صمم من ذات الشركة. يمكن أن يعمل النظام في شريحة على أنظمة تشغيل «ويندوز» أو «أندرويد»، حيث تم تصميم هذا النظام في شريحة واحدة للحصول على تكلفة تصنيع أقل وفي ذات الوقت التمكين لأنظمة تشغيل شبيهة بالحاسب الآلي في هواتف ذكية صغيرة.



■ شكل(٤): بعض مكونات النظام في شريحة.

ضم النظام في شريحة جميع مكونات الحاسب الآلي على دائرة إلكترونية متكاملة يصل حجمها (٢ملم×٢ملم) شكل (٤)، وتحتوي هذه الشريحة على دوائر رقمية، وتناظرية، ودوائر مختلطة وأحيانا ما يسمى بموجات الراديو. توصل هذه المكونات ببعضها وفق بروتوكولات، مسارات خاصة، أو متحكم للتواصل بين المكونات بعضها بالبعض الآخر، ومن هذه المسارات (AMBA bus) من شركة «ARM». كما يستخدم (DMA Controller) كواجهة لتوصيل البيانات بين الذاكرة ومنافذ التوصيل الخارجية، وغيره من البروتوكولات.

الجدير بالذكر أن العديد من الشركات تتنافس في تصنيع «نظام في شريحة»، و يتفاوت مستوى هذا التنافس من شركة لأخرى ومن عام



■ شكل (٥): صورة بالأشعة توضح مكونات «النظام في شريحة».

لآخر باختلاف دقة التصنيع التي تستخدمها الشركة والتي تكلفها الكثير من المال لمواكبة آخر تقنيات التصنيع، فمثلاً تستعين شركة أبل حاليا بمصانع شركة سامسونج في تصنيع الشرائح الخاصة بها فيما تنافسها شركة (TSMC) لأخذ التعاقد منها في المستقبل.

تمثل الأجزاء الرئيسة لهذا النظام، شكل (٥)، فيما يلي:

■ **المعالج (Processor)**: ويهدف لمعالجة العمليات وإرسال الأوامر لتنفيذ العمليات. و في بعض الأحيان تحتوي الشريحة على أكثر من معالج فيطلق عليها شريحة المعالجات المتعددة، حيث يكون لكل معالج غرض مختلف عن الآخر، كأن تكون هناك وحدة معالجة للرسوميات (GPU)، ووحدة المعالجة المركزية (CPU) وغيرها.

■ **شريحة الذاكرة (On-chip-memory)**: وهي ذاكرة مدمجة لقراءة وكتابة وتخزين البيانات. وتشمل (ROM, RAM, EEPROM, Flash memory).

■ **واجهات ومنافذ توصيل خارجية ذات معايير قياسية (USB, FireWire, Ethernet, USART, SPI)** لإرسال البيانات و استقبالها والتوصيل بالإنترنت.

■ **واجهات تناظرية (Analog and Digital interfaces)**: وتشمل (ADCs & DACs) وتعمل على تحويل الإشارات من رقمية (Digital) إلى تناظرية (Analog) والعكس، وتستخدم مثلا في استقبال الصوت عبر الميكروفون وإخراج الصوت عبر السماعات. كذلك واجهة لتوصيل النظام بالكاميرا (Camera Interface)، وواجهة الربط مع الشاشة (LCD Interface).

■ **دوائر إلكترونية لتنظيم الجهد وإدارة الطاقة.**

■ **ملحقات**: كالدوائر الإلكترونية التي تتحكم بتشغيل الجهاز ورفع الصوت وخفضه.

الهواتف الذكية في السوق

يؤثر تاريخ إصدار الجهاز وموعد نزوله السوق وثمنه على اقبال المستهلكين لذا يوجد تحد كبير في اختيار الموعد المناسب لإصدار الجهاز المناسب. حيث أن هناك تأثيرا للأجهزة التي ضمت مواصفات مستحدثة و وصلت إلى السوق قبل منافسيها ويكون الإقبال عليها كبيرا. يوضح جدول (١) قيمة تقريبة للتكلفة التصنيعية لجهازين في السوق الحالي يظهر فيهما أهم مكونات الهواتف المحمولة الذكية وتكلفتها الفعلية من قبل الشركة المصنعة.

خاتمة

تطورت وسائل الإتصال خلال الثلاثين عام الماضية حتى ظهر ما سُمّي بالهاتف المحمول الذكي والذي أصبح في متناول جميع شرائح المجتمع بمختلف أعمارهم، وقد تميز هذا الهاتف عن سابقه من الهواتف المحمولة بوجود الشريحة الأم التي أضافت لهذه الأجهزة مزايا مبتكرة ومواصفات مستحدثة أوجدت ذلك الفرق الكبير، كما تم التعرف على أهم المكونات الرئيسية في «النظام في شريحة» التي جعلت منه هذه القدرة فائقة الأداء محاكية لمتطلبات عمل الجهاز بأحدث التقنيات حتى شُبّه كثيرا بالحاسب الآلي المحمول.

من المتوقع ظهور أجيال أكثر ذكاء من سابقها كظهور هاتف محمول يقوم بشحن البطارية لاسلكيا، أو هاتف بسماكة الورقة مع عرض صور عالية الدقة على حائط الجدار، وغيره مما يستطيع الخيال تخيله.

التكلفة (بالدولار)		
المكونات	جهاز(١)	جهاز(٢)
الشاشة والزجاج	39.00	29.00
البطارية	6.00	3.50
الكاميرا	20.00	15.00
التوصيلات	13.00	8.00
منفذ الذاكرة NAND	11.00	15.00
ذاكرة SDRAM	9.00	5.00
المعالج	35.00	36.50
BB+XCR	24.00	25.50
إدارة الطاقة/الصوت	7.00	2.00
غير الكهربائية	11.00	9.00
أخرى	25.00	35.00
مواد مساعدة	5.00	5.50
التجميع والاختبار	9.00	10.50
الاجمالي	214.00	200.00

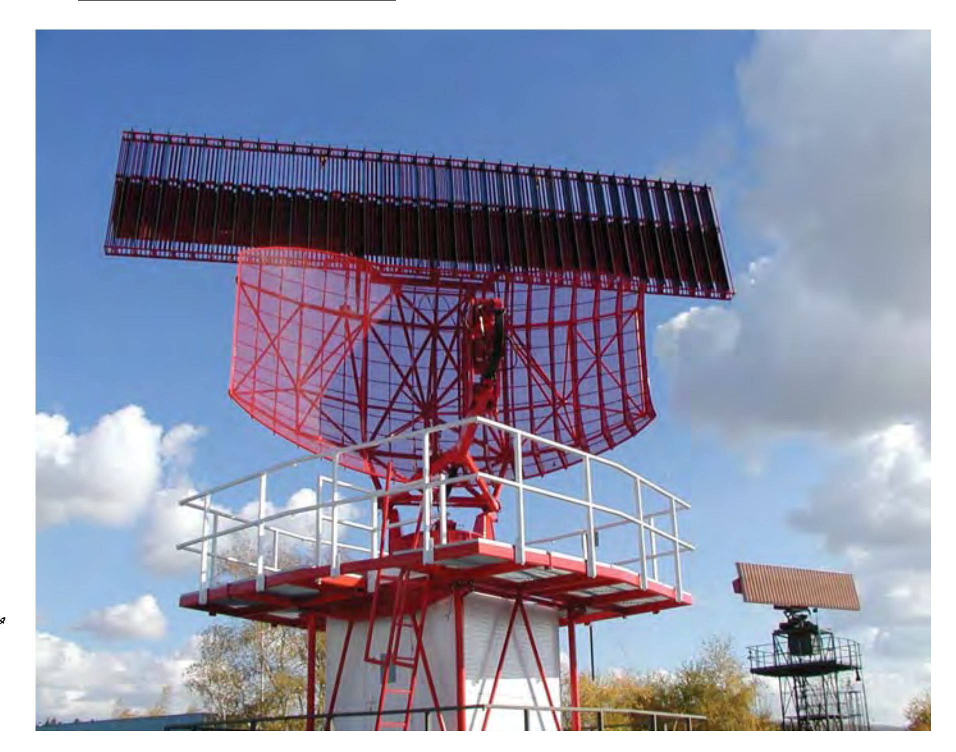
■ جدول (١): أهم مكونات الهواتف المحمولة الذكية لجهازين في السوق، وتكلفتها بالدولار، عام ٢٠١٣م.

المراجع

- Inside the Apple A7 from the iPhone 5s – Updated, Contributed by Dick Jame, September 27/2013 , chipworks.com/en/technical-competitive-analysis/resources/blog/inside-the-a7/
- Quick Turn Teardown of the Apple iPhone 5s, techinsights.com/apple-iphone-5s/
-Tech Insights Stacks Apple iPhone 5s vs. Samsung Galaxy Note 3, techinsights.com/iphone5s-vs-galaxynote3/

رادارات الاستطـلاع الثانويـة

د. حاتم بحيري و م. شريف نعمت



رادارات الاستطلاع الثانوية هي رادارات تستخدم تقنية تستطيع بوساطتها تحديد هُويّة الهدف هل هو صديق أم عدو؟ وهي بذلك تختلف عن الـرادارات الأساسيّة التي تُستخدم للكشف عن وجود هدف في الفضاء فقط. وقد استُخدمت أنظمة الرادار الثانويّة لأوّل مرّة أثناء الحرب العالميّة الثانية، ويعرف التطبيق العسكري للرادار الثانوي بتقنية تحديد صديق أم عدو، كما تُستخدم المعلومات المتحصّلة منه كمدخل في منظومة لاتخاذ القرار بإطلاق النار أو اتّخاذ إجراء ما ضد هدف عدو.

في عام ١٩٩٦م، قرّرت قيادة الأركان المشتركة في وزارة الدفاع الأمريكيّة أن تعتمد جاهزيّة طائراتها على استخدام أنظمة تحديد صديق أم عدو من ضمن متطلّبات أخرى لإقرار جاهزية الطائرة للقيام بمهمّات.

تُعتمد الخصائص التقنيّة لـرادارات الاستطلاع الثانوية على تحديد صديق أم عدو، وفقًا لوثيقة اتفاقية مقاييس باسم (STANAG-4193) التي وضعتها وكالة المقاييس في حلف دول شمال الأطلسي، (الناتو).

يتناول هذا المقال خصائص وأنماط رادارات الاستطلاع الثانويّة مقارنة بخصائص الرادارات الأساسية ومكوّناتها وكيفيّة عملها وتطبيقاتها.

مبدأ عمل الرادارات الأساسية والثانويّة

يعتمد مبدأ عمل الرادارات الأساسيّة على بث نبضة ذات طاقة عالية عبر الفضاء باتجاه هدف ما، ويكتشف الرادار وجود الهدف عندما ينعكس جزء من هذه الطاقة من على سطح ذلك الهدف. كما يمكن للرادار الأساسي أيضًا أن يستنتج مدى بُعد الهدف بحساب فارق الزمن بين وقت إرسال النبضة ووقت استقبال الانعكاس. من جانب آخر فإن الرادارات الثانويّة، تهدف إلى تحديد هُويّة هذا الهدف بشكل إيجابي وتمييزه من غيره بيقين، وليست معرفة وجود هدف ما أو حساب مدى بُعد ذلك الهدف.

في حالة الرادار الثانوي، فإنّ الهدف يجب أن يكون مزوَّدًا بجهاز إرسال استقبال خاص يُعرف بالمستجيب (Transponder -TxP) حتى يتم التعرف عليه، حيث يستقبل هذا الجهاز نبضات مُرمّزة – تعرف بالاستجوابات- من الطاقة على تردد ١٠٣٠ ميجا هيرتز، وهي تُولّد من جهاز إرسال استقبال خاصّ يعرف بالمستجوب (Interrogator -Int). بعد معالجة استجواب ما، يجيب المستجيب بإرسال نبضات مُرمزة تحتوي معلومات هُويّته على تردد ١٠٩٠ ميجا هيرتز، حيث يستقبل المستجوب الإجابة ويفسّرها ويحدّد هُويّة المرسل، ثم ينقل هذه المعلومة إلى شاشة عرض في التطبيقات البسيطة، أو إلى منظومة القيادة والسيطرة في النُّظم الأكثر تعقيدًا.



■ شاشة عرض الرادار.

العلاقة بين الرادار الأساسي والرادار الثانوي

يُستخدم الراداران: الأساسي والثانوي – عادة – معًا، كما تدور هوائياتهما بشكل متزامن في معظم الحالات. يستخدم الرادار الأساسي عادة لكشف وجود هدف ما في الفضاء، بينما يحدّد الرادار الثانوي ارتفاع وهُويّة هذا الهدف، كما يقرّر هل هو صديق أم عدو؟

في الأجواء المزدحمة بالطائرات، عادة ما تكون شاشات عرض الأهداف التقليديّة التي تعتمد على النقاط أو الومضات مكتظّة وممتلئة. كذلك هو الحال أيضًا مع شاشات عرض الحاسب الأكثر حداثة، خاصّة إذا كانت المعلومات المعروضة على الشاشة ناتجة فقط من الرادار الأساسي. في هذه الحالة يصبح من الصعب جدًّا ربط نقطة أو ومضة على الشاشة مع هدف في الفضاء، حتى لو كانت مسارات الطائرات معروفة مسبقًا لدى مراقب شاشة الرادار. يُعطي الرادار الثانوي معلومات إضافيّة من مُستجيب الطائرة، وإن تم ربط هذه المعلومات مع المعلومات الناتجة من الرادار الأساسي فإنّ هذا يسهّل كثيرًا عمليّة ربط النقاط مع الأهداف وتَتَبُّع هذه الأهداف على الشاشة.

نظرًا لطبيعة قناة الاتّصال ذات الاتجاهين في الرادار الثانوي – أي إرسال واستقبال، وليس إرسالاً وانعكاسًا كما في الرادار الأساسي – فإنّ الطّاقة اللّازمة لإرسال استجواب في حالة الرادار الثانوي أقلّ بكثير من الطّاقة اللّازمة لإرسال نبضة في رادار أساسيّ يعمل على مدى التغطية نفسه. كما تجدر الإشارة أن مشكلات صدى قنوات الاتصال وكثير من الانعكاسات غير المرغوبة يتم تجنّبها في الرادارات الثانويّة لأنّ المُرسل والمُستقبل يعملان على تردّدات مختلفة، و عليه فإنّ تكلفة رادار ثانوي تمثّل جزءًا صغيرًا من تكلفة رادار أساسيّ يعمل على مدى التغطية نفسه.

الأجزاء الرئيسة للرادار الثانوي

يتكوّن الرادار الثانوي، شكل (١) من الأجزاء الآتية:-

- **الهوائيّات**

عادة ما تُزوّد المستجوبات بهوائيّات موجّهة، بينما المستجيبات عادة ما تستقبل وتجيب باستخدام هوائيّات متعدّدة الاتجاهات.

- **المستجيب**

المستجيب عبارة عن جهاز إرسال استقبال يمتلك القدرة على استقبال الاستجوابات من المستجوب ليعالجها، ومن ثم يرسل الرد المناسب.

- **المستجوب**

المستجوب عبارة عن جهاز إرسال استقبال يستطيع إرسال الاستجوابات واستقبال الإجابات من عدد كبير من المستجيبات المثبتة على أهداف. عادة ما يستطيع المستجوب معالجة إجابات ١٥٠٠ هدف في الوقت نفسه، حيث يعالج هذه الإجابات ليحدد هُويّة، موقع ومدى الأهداف.

- **أجهزة التشفير**

تمكّن هذه الأجهزة المستجوِب والمستجيب من التواصل بشكل آمن في التطبيقات العسكريّة.

- **شاشة العرض**

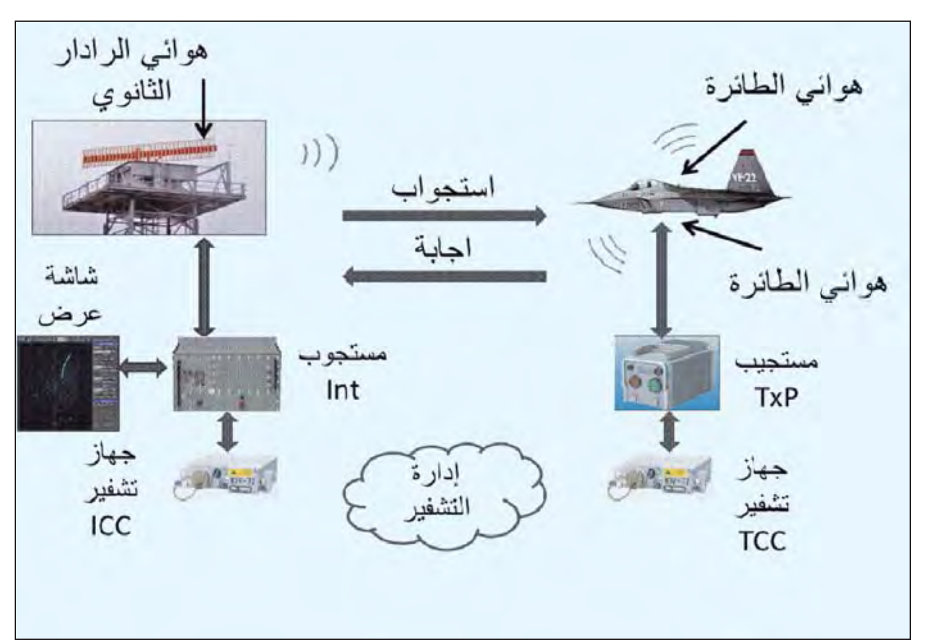
تستخدم شاشة العرض لرصد الأهداف باستخدام المعلومات المستقبلة من الرادار الثانوي، أو من الرادار الأساسيّ أيضًا.

- **إدارة التشفير**

إدارة التشفير عبارة عن آلية لتبادل مفاتيح التشفير، لتمكين أجهزة التشفير من العمل في المنظومة بالشكل الصحيح.

أنماط عمل الرادارات الثانوية

نمط العمل هو الطريقة التي تتم بها عملية الاستجواب بين المستجوَب والمستجيب. يوجد في العالم حاليًّا سبعة أنماط شائعة الاستخدام في الرادارات الثانوية، هي الأنماط: (1،2)، (4،5)، (A\3،C)، و (S)، حيث تستخدم المنصّات العسكريّة الأنماط: (1، 2)، (C،4\3)، (A)، و (5)، بينما تستخدم المنصّات المدنيّة أنماط: (C)، (A)، و (S) تعرف الأنماط (1، 2) و (3) بأنماط تعريف الهُويّة (Selectivity Identification Feature –SIF- modes). يتم استخدام النمط (S) تدريجيًّا بشكل متزايد لإستبدال أنماط ال (SIF) في دول العالم، لكن على الرغم من ذلك، فلا تزال دول عديدة تستخدم أنماط ال (SIF) فقط.



■ شكل (١) الأجزاء الأساسية لأنظمة الرادارات الثانوية.

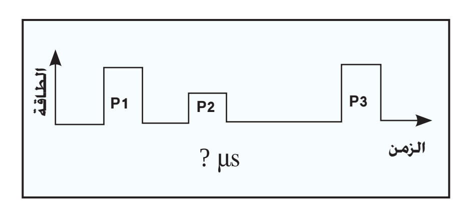
يمكن تلخيص الخواص الزمنيّة الرقميّة لجهاز المستجيب وعلاقتها بأنماط عمل الرادارات الثانوية. وفقًا لوثيقة الناتو (STANAG-4193) وفقًا لما يلي:-

● **استجوابات الرادارات الثانويّة**

تعرَف النبضات الصادرة من المستجوب بالاستجوابات. يستقبل المستجيب هذه الاستجوابات في الأنماط: (1 ،2)، (A\3) و(C) على هيئة ثلاث نبضات تسمّى (P1)، (P2) و (P3). كما هو موضّح في شكل (٢).

يحدّد نمط الاستجواب وفقًا للمدّة الزمنيّة بين النبضة الأولى (P1) والثالثة (P3) ، كما هو مبيّن في جدول (١) وبناء على ذلك تُعرَف المعلومات التي يطلبها المستجوب من مستجيب الهدف. أمّا النبضة (P2) فهي نبضة قمع المناطق الجانبيّة في هوائي المستجوب، وسوف تجري مناقشتها لاحقًا.

يُستخدم النمطان: (1) و(2) في التطبيقات العسكريّة لطلب رقم هُويّة الهدف ورقم مهمّته، وتُخصّص هذه الأرقام للأهداف الجهة المسؤولة في القوات المسلّحة، كما يمكن لطاقم الصيانة أو الطيّار أو غيرهم برمجتها على المستجيب قبل بدء المهمّة. فيما يتعلّق بالنمط (A\3) فإنه



■ شكل (٢) نمط استجواب غير مشفر في أنظمة الرادارات الثانوية.

المستخدم	المدة الزمنية بين P1-P3 (μs)	نمط الاستجواب
عسكري	٣	1
عسكري	٥	2
مدني/ عسكري	٨	A\3
عسكري	٢١	C

■ جدول (١): تلخيص أنماط الاستجواب غير المشفَّرة في أنظمة الرادارات الثانوية.

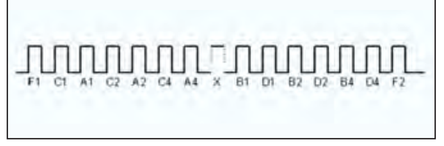
يستخدم مدنيًا في تطبيقات الملاحة الجويّة، وعسكريًّا لتحديد هُويّة بعض الأهداف. أمّا النمط (C) فإنّه عادة ما يستخدم مدنيًّا في تطبيقات الملاحة الجويّة لطلب ارتفاع الهدف عن سطح البحر حيث يتم تحديد الارتفاع بوساطة جهاز قياس ضغط الهواء منفصل عن المستجيب، حيث يُرسل معلومات الارتفاع للمستجيب الذي يرسلها - بدوره- للمُستجوب عند الطلب.

● **إجابات أنظمة الرادارات الثانوية**

يوضح الشكل (٣) شكل الإجابة غير المشفّرة لأنظمة الرادارات الثانوية. حيث تُستخدم النبضتان: (F1) و (F2) اللتان تكونان- دائمًا- موجودتين في أيّ إجابة لتحديد الإطار الزمني للرد، وتكون عادة في بداية ونهاية الإجابة. كما يقع بين نبضتي الإطار ١٣ نبضة بيانات، واحدة منها غير مستخدمة، وهي النبضة المسماة (X) الموضّحة في الشكل (٣)، ما يترك ١٢ نبضة تسمح بـ (٤٠٩٦) حدٌّ أعلى من تركيبات الإجابات الممكنة، حيث يستخدم كلّ نمط من أنماط الإجابة جميع النبضات الـ ١٢ أو جزءًا معيّنًا منها.

● **إجابات مؤشّر الموقع الخاص، وإجابات الطوارئ غير المشفرة**

قبل ظهور شاشات الرادار الحديثة - عندما كانت تواجه مراقب شاشة الرادار مشكلات بصريّة عند محاولة تتبع هدف ما - فإنّه كان غالبًا ما يلجأ للطلب من قائد هذا الهدف خصّيصًا تشغيل، مؤشّر خاصّ لمدّة معيّنة حتى يستطيع تفرقته عن غيره، ثم يطلب منه إيقاف تشغيله. حيث يمكن لمُشغّل المُستجوب أن يطلب من قائد هدف ما- عبر قناة اتصال



■ شكل (٣) هيئة الإجابة الاعتيادية غير المشفَّرة لأنظمة الرادارات الثانويّة.

صوتية مثلًا- أن يشغّل مفتاحًا خاصًّا في قمرة القيادة يسمّى مؤشر الموقع الخاص (Special Position Indicator -SPI). يرتبط هذا المفتاح مباشرة بالمستجيب، وعندما يكون في وضع التشغيل فإنّ المستجيب يدعم الإجابة بهذه الخاصيّة. تكون إجابات مؤشّر الموقع الخاصّ مدعومة في الأنماط (1 ،2) و(A\3). ففي حالة نمط ١، تتكوّن إجابة المؤشر الخاص من إجابتين متتاليتين من إجابات نمط ١ بينهما مدّة تأخير ثابتة. أمّا في حالة النمط (2) و(A\3) فإنّ نبضة زائدة ترسل بعد نهاية الإجابة المعتادة لهذه الأنماط. (مع تطوّر شاشات الرادار وأنظمة تعقّب الأهداف لم يعُد هذا المؤشر يستخدم بكثرة في العصر الحاضر).

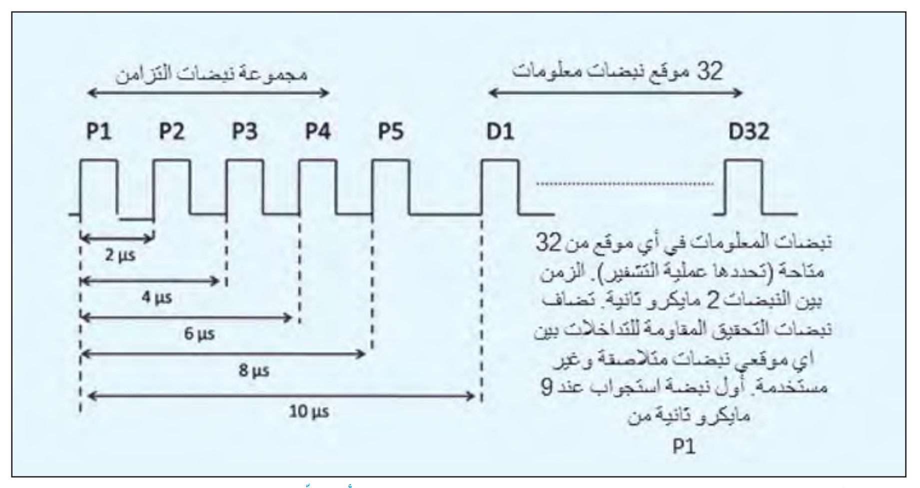
أمّا في حالة إجابات الطوارئ في الأنماط (1)، (2) و(A\3)، التي تشير إلى حالة طارئة لدى الهدف وأنّ مؤشر الطوارئ المربوط بالمستجيب قد شغّله قائد الطائرة، فإن الإجابة الناتجة عن تشغيل هذا المؤشر هي إجابة اعتياديّة غير مشفّرة - كما في الشكل (٣) - متبوعة بثلاث مجموعات من نبضات الاطار (F1) و (F2).

● **تمييز الصّديق من العدوّ**

يمكن تمييز الصّديق من العدوّ باستخدام النمط (4)، وهي طريقة تمكّن جهاز المستجوب من تحديد الأهداف الصديقة بيقين. حيث تمّ تضمين خواص أمنيّة إضافيّة إلى آلية الاستجواب/ الإجابة في النمط (4)، ما يحدّ من إمكانيّة تقمّص هدف عدوّ لهُويّة هدف صديق التي يمكن حدوثها في الأنماط الأخرى غير المشفّرة.

● **الاستجواب في النمط (4)**

تختلف عمليّة الاستجواب المستخدمة في النمط (4) عن عمليّات الاستجواب في الأنماط الأخرى غير المشفرة، حيث يتلقّى جهاز المستجيب عند استخدام النمط (4) إشارة مكوّنة من سبع وثلاثين نبضة مقارنة بإشارة مكوّنة من ثلاث نبضات فقط، في حالة استخدام الأنماط الأخرى غير المشفّرة كما هو موضح



■ شكل (٤): الرسم البياني للتوقيت في الاستجواب المشفر لتحديد صديق أم عدو.

في شكل (٤). تُعرف الأربع نبضات الأولى «بمجموعة نبضات التزامن»، فيما تعرف النبضة الخامسة بنبضة «قمع المناطق الجانبيّة» كما سوف يُناقش في قسم خاص أدناه. أمّا الاثنان وثلاثون نبضة المتبقيّة في الإشارة المرسَلة فهي عبارة عن رسالة مشفّرة يتم تكوينها في جهاز التشفير المتّصل بجهاز المستجوب (Interrogator Crypto Computer-ICC). و تحتوي هذه الرسالة مدّة التأخر في الرد التي يجب على جهاز المستجيب انتظارها قبل البدء بإرسال الإجابة لعمليّة الاستجواب من النمط (4)، ومن ضمن المُدخلات التي يمكن اختيارها لجهاز التشفير المتّصل بجهاز المستجوب أو لجهاز التشفير المتّصل بجهاز المستجيب (Transponder Crypto Computer- TCC) في حال استخدام النمط (4)، هي إشارة لاختيار مجموعة مفاتيح الشيفرة من بين مجموعتين من المفاتيح تكون مضمّنة مسبقًا في الجهاز (الرمز أ/ب) كما يمكــن تعديل استخـدام تلك الإشارة كي تستخدم لأغراض أخرى من قِبل مصمّمي جهاز التشفير.

● الإجابات في النمط (4)

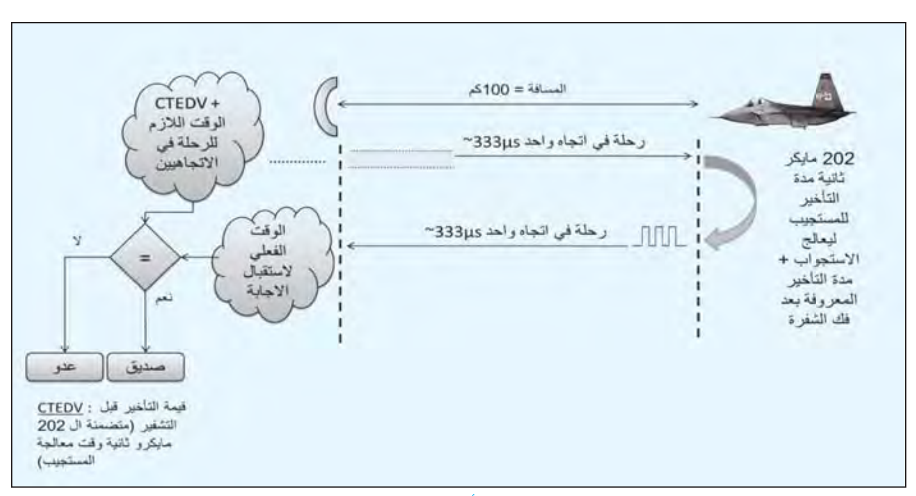
يجيب جهاز المستجيب على عملية الاستجواب بصيغة ثلاث نبضات، شكل (٥)، فإذا أرسل الهدف عددًا معيّنًا أو نسبة معيّنة من الإجابات المتأخّرة زمنيًّا تكون مطابقة لقيمة التأخّر في الرد المُستنتجة من عملية فكّ تشفير التحدّي المرسلة من جهاز المستجوب خلال عملية الاستجواب، فإنّ جهاز المستجوب سوف يصنف ذلك الهدف كصديق، وكنتيجة لذلك سوف يتم عرض الهدف كصديق على شاشة الرادار.

تُجمع قيمة التأخر في الرد المستنتجة عن عملية فك تشفير الاستجواب المذكورة سابقًا مع قيمة تأخّر ثابتة (٢٠٢ مايكرو ثانية من وقت وصول النبضة (P4) لجهاز المستجيب التي هي آخر نبضة في مجموعة نبضات التزامن) لتحديد القيمة النهائيّة للزمن الذي يجب على جهاز المستجيب انتظاره قبل البدء بإرسال أيّ رد. تعطي هذه القيمة الثابتة للتأخير جهاز المستجيب وقتًا كافيًا لتمرير الاستجواب إلى جهاز التشفير المتّصل بجهاز المستجيب المتصل به لفكّ التشفير. تعطي آلية التأخير المستخدمة- أيضًا- جهاز المستجوب وقتًا كافيًا للتأكّد من مدى بُعد الهدف بدقّة، التي تتم بناءً على الوقت الدقيق لوصول الرد من الهدف كما هو موضّح في شكل (٥). خلال عمليّة دوران الهوائيّ المتّصل بجهاز المستجوب، وفي أثناء تعرّض الهدف للإشارات المرسلة، يمكن أن تتكرّر العمليّة الموضّحة بالصورة عدّة مرّات، بناء على عدّة عوامل، مثل: سرعة الهدف، والوقت المستغرق خلال دورة كاملة للهوائي، بُعد الهدف و عدد المرات التي يرسل فيها المستجوب استجوابات في الثانية الواحدة. كما يعتمد عدد المرّات التي يجب أن تتكرر العملية المذكورة أعلاه فيها- قبل أن يتم تصنيف أيّ هدف كصديق- على تصميم جهاز المستجوب.

تتكوّن الإجابة المرسلة من جهاز المستجيب كردّ على عملية استجواب من النمط (4) من مجموعة مكوّنة من ثلاث نبضات، كما هو موضّح في شكل (٥)، إلا أنّ شكل النبضات المستلمة لا يشكّل أهميّة عظمى، لكن المهم هو استخدام التوقيت الصحيح.

● نبضات الاستجوابات المقاومة للتداخلات

لا يُستخدم الاثنان وثلاثون نبضة أو مواقع النبضات على الدوام، بل يعتمد استخدامها من عدمه على قيمة الرسالة المشفرة. وتنص وثيقة (STANAG-4193) على أنّ نبضات استجواب



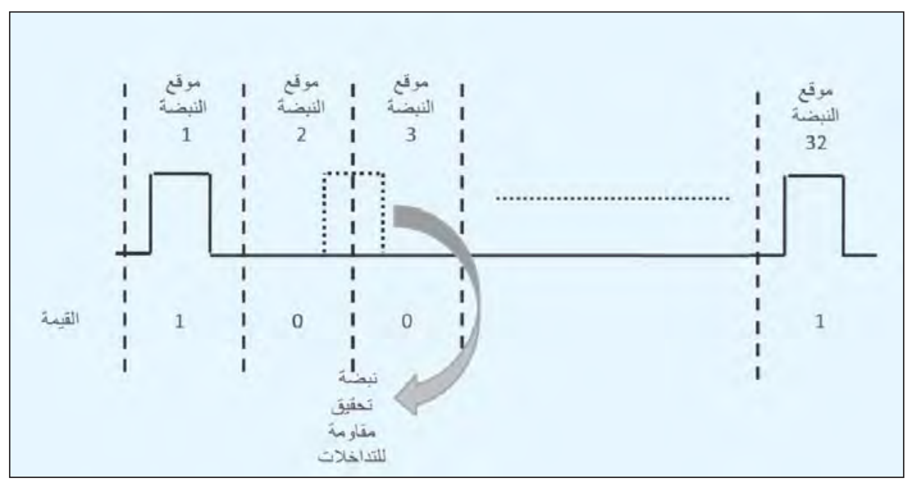
■ شكل (٥) مثال على إجراءات عملية التحقق من صديق أم عدو في النمط (4).

مقاومة التداخلات يجب أن تدخل بين أيّ موقعي نبضات متلاصقة وغير مستخدمة في مجموعة نبضات المعلومات. تساعد هذه النبضات على تقليص تداخل إشارات استجواب من أجهزة استجواب أخرى قد تكون في الجوار، شكل (٦).

● **قمع المناطق الجانبيّة الناتجة عن جهاز المستجوب**

يُعدُّ تصميم هوائي جهاز المستجوب غير مثاليّ، وقد يقود إلى توليد إشارات مناطق جانبيّة غير مرغوب بها، وعليه لا تردّ أجهزة المستجيب إذا كانت في منطقة تكون فيها انبعاثات المناطق الجانبيّة من الهوائي عالية، لأنّ ذلك قد يقود جهاز المستجوب للاعتقاد خطًا بوجود هدف في اتّجاه البثّ الأساسي، ولحلّ تلك المشكلة، فإنّ جهاز المستجوب يرسل نبضة عالية الطاقة (أعلى من النبضات الأخرى) من هوائي منفصل في اتّجاه المناطق الجانبيّة لهوائي الإرسال الرئيس لإبلاغ جهاز المستجيب بوجوده في منطقة جانبيّة، وعليه عدم الرد على أيّ إشارات استجواب مُستلَمة. تدعى هذه العملية «قمع المناطق الجانبيّة الناتجة عن جهاز المستجوب».

يوضح شكل (٧) أنّ جهاز المستجوب الملحق بهوائيات للأنماط (2)، (1)، (A/3) و (C)، يبث نبضات (P1) و(P3) باستخدام الهوائي الموجّه الرئيس، فيما يبث النبضة (P2) باستخدام هوائي



■ شكل (٦) سيناريو محتمل لاستخدام نبضات الاستجواب المقاومة للتداخل في نمط (4) المشفر.

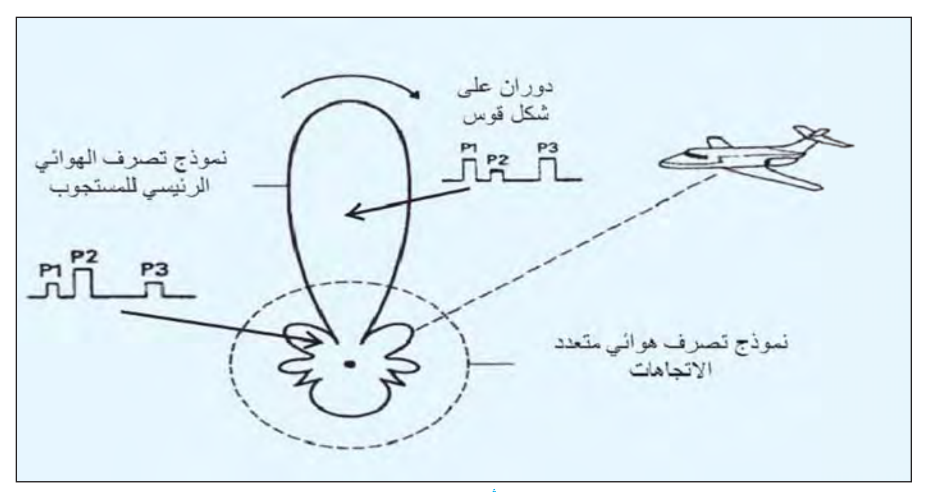
متعدّد الاتجاهات منفصل. في حالة استخدام المستجوب في نمط (4) المشفر، فإنّ الإشارة (P2) تبث من الهوائي الموجّه الرئيس، وذلك لقمع أجهزة المستجيب غير المهيأة للردّ باستخدام النمط (4).

النمط الوطني الآمن

الهدف الرئيس لأجهزة أنظمة تحديد الصديق من العدوّ المستخدمة على متن المركبات والمعدّات في جميع أفرع القوّات المسلّحة، مثل: الطائرات ومحطات الرادار، هو تبادل المعلومات المعروفة لها. تأخذ هذه المعلومات شكل استجوابات وإجابات، وتحرص معظم الدول على امتلاكها لنظام عسكري لتحديد الصديق من العدوّ باستخدام نمطها الخاص الذي يستخدم تقنيات التشفير لضمان أمن وسريّة الاستجوابات والرّدود، وعدم إمكانية استغلال الخصوم لها.

المراجع

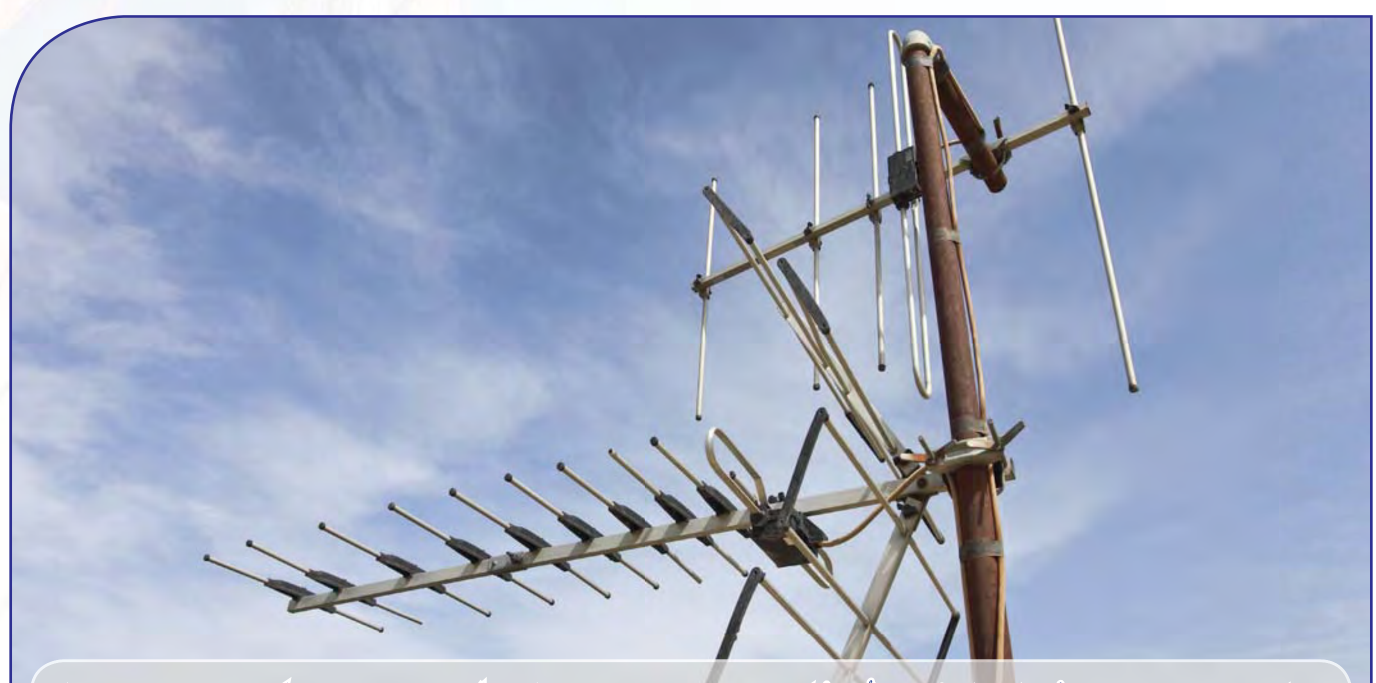
- "Identification Friend or Foe" [Online] Available: http://www.globalsecurity.org/military/systems/aircraft/systems/iff.htm (Accessed in June 2010).
- Kingsley. S. and Quegan, S. (1999). Understanding Radar Systems. SciTech Publishing.
- Military Agency for Standardization, North Atlantic Treaty Organization (NATO). (1990). Standardization Agreement (STANAG) 4193 PART 1 edition 2 Annex A and appendices, Technical Characteristics of IFF - Mk XA and Mk XII Interrogators and Transponders.
- Sharef Neemat (2010). Design and Implementation of a Digital Real-Time Secondary Surveillance Radar/Identification Friend or Foe Target Emulator. MSc Thesis. University of Cape Town.
- Stevens, M.C. (1988). Secondary Surveillance Radar. Artech House.
- United States Navy, Naval Air Systems Command and Naval Air Warfare Centre. (1999). Electronic Warfare and Radar Systems Engineering Handbook Rev 2.



■ شكل (٧) مثال على تصرف الهوائيات في المستجوب في أنظمة الرادارات الثانوية. الطائرة التي تكون في الشعاع الرئيس سوف تستقبل (P2) ذات طاقة أقل من باقي النبضات، ولذلك يُرد على الإستجواب.

مصفوفة الهَوائيّات المُضَعّفة

م. عبد الرّحمن محمّد بن غنام



الهَوائيّ (Antenna) هو قطْعة مَعْدنيّة مُوْصلة تُستخْدَم لالتقاط الإشارات اللاسلكيّة وبثّها، وعند استقباله المَوْجات الكهرومغناطيسيّة يُحَوِّلها إلى تيّار كَهْربائيّ، والعكسُ عند الإرسال، وتتفاوت أنواع الهَوائيّات من حيث الحجم وتكلفة التّصنيع ومقاييس الكفاءة.
تُستخدَم الهوائيّات في جميع الأنظمة اللاسلكيّة، مثل البثّ الإذاعيّ والتّلفزيونيّ، والاتصالات اللاسلكيّة المُباشَرة بين نقطتين، وشبكات تبادل البيانات المَحليّة اللاسلكيّة، وأنظمة الرّادار، وتلسكوبات استكشاف الفضاء، وتختلف الهَوائيّات حسب استخداماتها؛ فمنها ما يُستخدَم في الجوّ -يمثّل الاستخدام الأكبر- ومنها ما يُستخدَم تحت سطح الماء، كما تُستخدَم أيضًا في استكشافات التّربة والصّخور عند تردُّدات مُعَيّنة لمسافات قصيرة.

تتعدّد أنواع الهَوائيّات وتختلف مُمَيّزات بعضها عن بعض، مثل: هوائيّ الشريط الدقيق (Micro strip antenna) وهوائيّ الطّبَق (Dish antenna) والهوائيّ ثُنائي القُطب (Dipole antenna) ... الخ. يُستخدَم كُلٌّ من هوائيّ الشّريط الدقيق والهوائيّ ثنائي القطب بصورةٍ شائعة؛ لقلّة تكلفتها في صناعة الهواتف النقّالة، في حين يُستخدَم هوائيّ الطّبَق لاستقبال الإشارات القادمة من الأقمار الاصطناعية؛ وذلك لقدرته على استقبال الإشارات الضّعيفة؛ إذ إنّ الإشارات تصل إلى سطح الأرض ضعيفةً بعد مرورها بمسافات طويلة. يوضّح الشكل (١) نموذجًا لهوائيّ الشريط الدقيق، وآخر لهوائيّ الطبق.



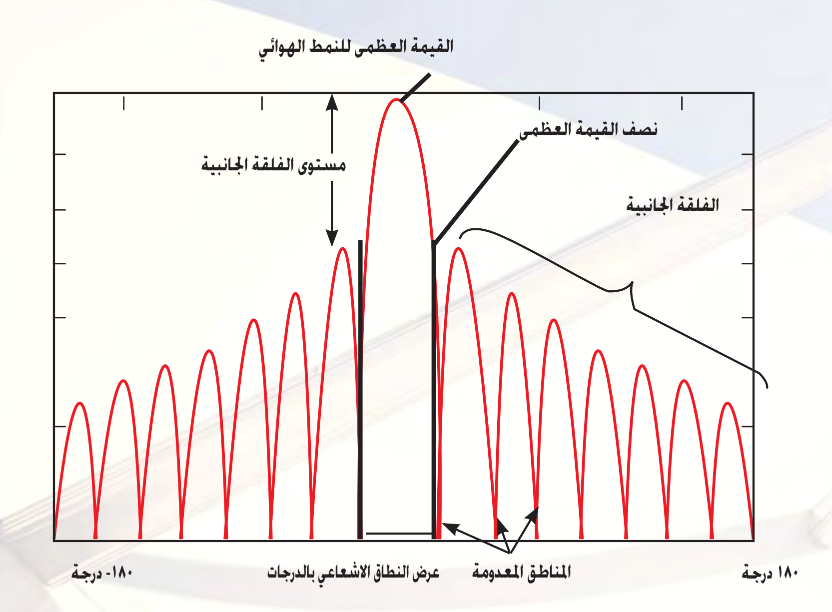
▪ شكل (١): هوائيّ الشريط الدقيق وهوائيّ الطبق.

النّمط الهوائيّ

يُمثل كلّ هوائيّ بنمطٍ هوائيّ لتقييم كفاءته، ويمكن توضيح النّمط الهوائيّ بأنه وَصْفٌ لمجال انتشار الإشارة المُرسَلة في الفضاء، ويُمثَّل على شكل بياني بدلالة الدرجات الزاوية، ويوضّح الشكل (٢) خصائص النّمط الهوائيّ (مجال واحد فقط) والذي يتكوّن من الأجزاء الآتية:

- النّطاق الإشْعَاعيّ الأساسيّ

يُمثّل النطاق الإشعاعي الأساسي (Main lobe) الجزء الأكبر من النمط الهوائيّ



▪ شكل (٢): خصائص النّمط الهوائي.

الذي يُعَبِّر عن الاتّجاه الفعلي للاستقبال و الإرسال.

- **القيمة العُظْمى**

تُمثِّـل القيمة العظمى المُوضَّحة – في قمّتها – معامل التكبير (Gain) لطاقة الإشارة المُستقبلة أو المُرْسلة.

- **عَرْض النّطاق الإشعاعي بالدرجات**

يُطلَـق عَرْض النطـاق الإشعاعي على عَرْض المنطقة المَحْصورة بـين النقطتين المُتناظِرتين في النّطاق الإشعاعيّ الأساسيّ، التي تَكُون فيها قيمة النّمط الهوائيّ نصفَ القيمة العظمى.

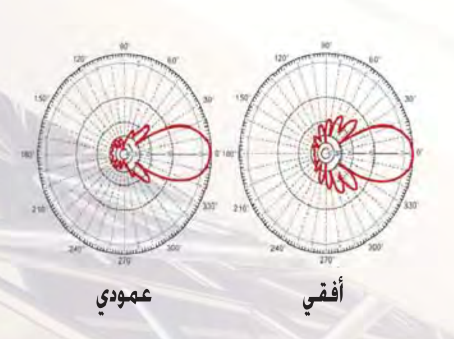
- **الفلقة الجانبيّة**

الفلقــة الجانبيّــة (Side lobe)، هي الجزء المجاور للنطاق الإشعاعيّ الأساسيّ من الجهتين، وهـو جزء غير مرغوب فيه؛ إذ إنّ كفاءة الهَوائيّ تتحسّـن كلما انخفض مستوى الفلقـة الجانبية مقارنـة مـع قيمة النّطـاق الإشْعاعـيّ الأساس، وبذلك يمكن تمثيل كفاءة الهوائيّ بمستوى الفلقة الجانبيّة، شكل (٢).

- **المَناطق المَعْدومة**

تُعَـرَّف المَناطـق المعدومـة (Nulls) بأنّهـا النقاط التي تَنْعَدِمُ فيها رؤية الهوائيّ.

يوضّح الشـكل (٣) النمط الهَوائـيّ المُتَكَوِّن من عنصرٍ هوائيٍّ وحيد، ويمكن تمثيله بمعادلات رياضيّة؛ إذ إنّه يصوِّر انتشار الإشارة اللاسلكيّة بصـورة ثلاثيّة الأبعـاد في الفضـاء، مُتكوِّنة من مجالـين متعامديـن، همـا: المَجـال الكهربائيّ، والمَجـال المغناطيسـيّ؛ أحدُهمـا أفقـيٌّ و الآخـرُ عموديٌّ؛ لتسهيل تخيّلها.



▪ شكل (٣) : نمط هوائيّ لعنصر هوائيّ وحيد.

▪ شكل (٤): مصفوفة الهَوائيّات المُتوافقة في الطَّوْر.

مصفوفة الهَوائيّات المُتوافِقة في الطَّوْر

تتألَّف مَصفُوفة العناصر الهوائيّة المُتوافِقة في الطَّـوْر (Phased antenna array)، شـكل (٤)، من مجموعة من هَوائيّات مُتماثلة مَفْصولة عـن بعضهـا بعضًـا بمسافـة ثابتـة ومُرَتَّبة على صورة صـفّ لتشكل هوائيًّا واحدًا؛ بحيث تُوَصَّلُ العناصر جميعهـا بجهاز الإرسـال أو الاستقبال (عناصر نشطة).

تقـدّم هـذه المصفوفـة – بمجملها – نمطًا هوائيًّـا ذا نطاق إشعاعـيّ عَرْضُه أقلُّ من عرض النّطاق الهوائيّ للعنصـر الواحد، ومعامل تكبير أعلـى للنطـاق الإشعاعـيّ الأساسـيّ، إضافـة إلى زيـادة مستـوى الفلقـة الجانبيـة؛ بحيث تَكُـون فعّالـة في التطبيقـات العسكريـة، مثـل الهوائيّـات المُستخدَمة في أنظمـة رادارات التّتبُّع (Tracking Radar System).

يمكن حساب كمّيّة طاقة النمط لمصفوفة هوائيّات مُتوافقة الطور رياضيًّا بمعلومية النّمط الهوائيّ الواحد، وعدد عناصرها طبقًا للمعادلة الآتية:

$$\textit{Array pattern} = \textit{single antenna pattern} \sum_{i=1}^{N} w_i e^{-jk.r_i}$$

حيث:

Array pattern	النمط الهوائيّ للمصفوفة
Single antenna pattern	النمط الهوائيّ لعنصر وحيد
N	عدد عناصر المصفوفة التي تُعَدّ بـ (i) لكلّ حدود المتسلسلة
wi	معامل يُعبِّر عن طور (Phase) كلّ عنصر (i)
k	الطول المَوْجيّ للإشارة المتوسّطة التردد 2π/λ سواء أكانت مرسَلة أم مستقبَلة
J	الجذر التّربيعي لسالب واحد

مصفوفة العناصر الهَوائيّة المُضعّفة

تُمثّل مصفوفة العناصر الهوائيّة المُضعّفة (Thinned antenna array) حالةً خاصّةً لمصفوفة الهّوائيّات المُتوافقة في الطور، وتقوم فكرتها على عزل بعض العناصر الهوائيّة عن جهاز الاستقبال والإرسال، وذلك بوصله بمقاومة (٥٠ أوم) ومن ثَمّ تأريضه (Grounding)، مع العلم أنّها تَتسبّب في فقد بعض الطاقة وتقليل معامل التكبير للنطاق الإشعاعيّ الأساسيّ للهوائيّ؛ بحيث تُعَدُّ بعضُ العناصر في المصفوفة المُضَعّفة عناصرَ غيرَ نَشطة (Inactive elements)، بعد أن كانت جميعًا عناصرَ نشطةً (Active elements) كما يتّضح في مصفوفة العناصر المضعفة في الشكل (٥).

تُقدّم مصفوفة العناصر المُضعَّفة نتائجَ فُضلى موازنةً مع مصفوفة العناصر الهَوائيّة المُتوافقة في الطّور؛ (نطاقًا إشعاعيًّا أضْيَقَ، ومستوىً أعلى للفلقة الجانبيّة مع وجود فقد في الطاقة)؛ لدعم أيّ نظام يحتاج إلى هوائيٍّ ذي نطاقٍ إشعاعي أضْيَقَ، مثلُ أنظمة رادارات التّتبُّع التي تتطلّب دقّةً مُتناهيةً في تحديد موقع الأهداف المطلوبة، ومُتابعة مُناورَتها.

● تطبيقات مَصفوفة الهَوائيّات المُضَعَّفة

تَمْلِكُ القواعدُ العسكريّة جميعها رادارَ بَحْث (Search radar) ورادارَ تتبّع (Tracking radar)؛ إذ يَكْشفُ رادارُ البَحْث عن فضاء المَنطَقة المُحيطَة بالقاعدة، وعند اكتشافها مَرْكَبةً مُريبةً غير صَديقة (طائرة أو سفينة أو دَبّابة) فإنّها تنبّه رادارَ التتبّع بوجودها وموقعها بصورة تقريبيّة؛ ليتابعَها هو ويقصفها إن دعت الحاجة. وتُعَدّ مصفوفة الهّوائيّات المُضَعّفة مناسبةً للعمل بصفتها جزءًا من نظام رادارِ التتبّع، الذي يُرَكِّز اهتمامَه في حيّزٍ صغيرٍ؛ لمتابعة الهدف، مثل طائرة حربيّة. يوضّح شكل (٦) الفرقَ بين رادار التتبّع ورادار البحث؛ إذ شُبِّهَا بكشّافين؛ أحدُهما (العُلْويّ) يضيء نطاقًا واسعًا من الفضاء، والآخر (السُّفْليّ) يضيء نطاقًا ضيّقًا (رادار التتبّع).



■ رادار بحث في قاعدة عسكرية.

● نموذج مصفوفة هوائيّة مُضَعَّفة

يمكن تصميم مصفوفة العناصر الهوائيّة المُضَعّفة لتقديم نطاقٍ إشعاعيّ أضيق، ومستوى أقلّ للفلقة الجانبية من خلال مرحلتين رئيستين، هما:

■ **المرحلة الأولى**: وتمثّلت في اكتشاف توزيع مُناسِب للعناصر النّشطة وغير النّشطة (تُسَمَّى الشّفرةَ الثّنائيّةَ) في المصفوفة؛ باستخدام كتابة ملفٍّ مُبَرْمَج ببرنامج الماتلاب (Matlab)؛ لكشف عدّة خيارات مُناسبة تؤدّي المطلوب باستخدام الخوارزميّة الجينيّة (Genetic Algorithm)، وطريقة تحسين السّرب الجزئيّ (Particle Swarm Optimization) للحصول على أفضل النتائج المُمكنة باستخدام آليّات معيّنة لاكتشاف شيفرة ثنائية (عدد الأرقام الثنائية نفسها عددُ العناصر الهوائية) تحقّق قيمةً مَعقولةً؛ لعرض النطاق الإشعاعي، ومستوى الفلقة الجانبي، وتُسَمَّى الجين (Gene). حيث اُسْتُخْرِجَتْ تصاميم مُرَشّحَة؛ لبنائها في المختبر.

■ **المرحلة الثانية**: وتمثّلت في تنفيذ التّصاميم المُكتشَفة في المختبرات، وبناء مَصفوفة هوائيّة؛ لقياس النمط الهوائيّ عمليًّا، وموازنته مع

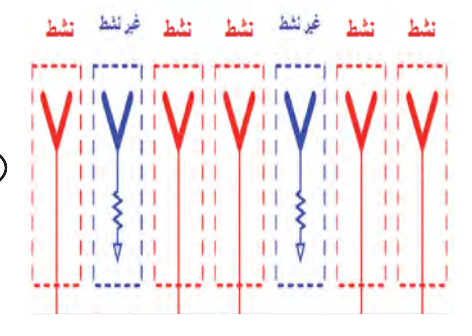
رادار البحث

كشاف يضيئ منطقة واسعة، لذا فدقة كشفه للجزيئات الصغيرة غير فعالة

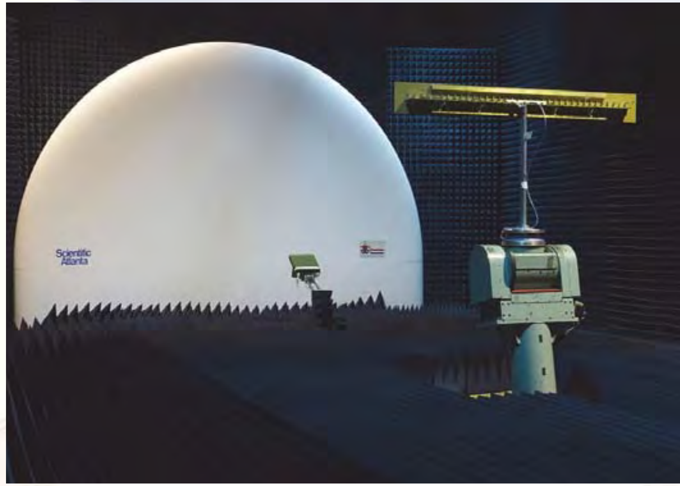
رادار التتبع

كشاف يضيئ منطقة ضيقة، لذا هو دقيق وفعال في كشف الجزيئات الصغيرة في نطاق رؤيته بسبب تمركز الضوء في نطاق ضيق

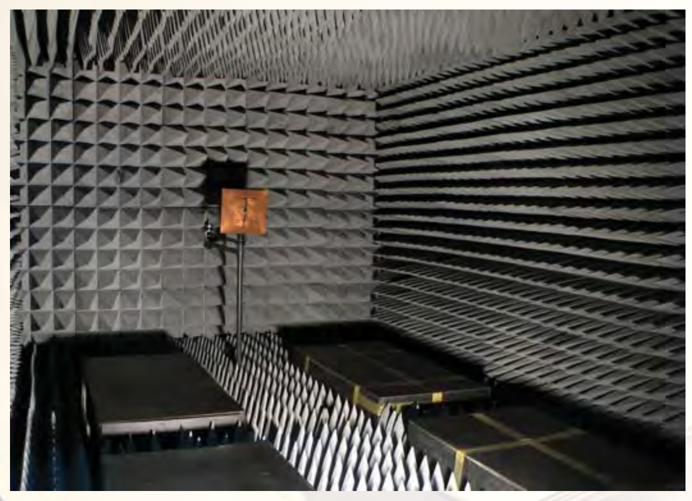
■ شكل (٦): تمثيل راداريَ البحث والتّتبّع على صورة كَشّافيْن.



■ شكل (٥) : مصفوفة الهوائيّات المُضَعَّفة



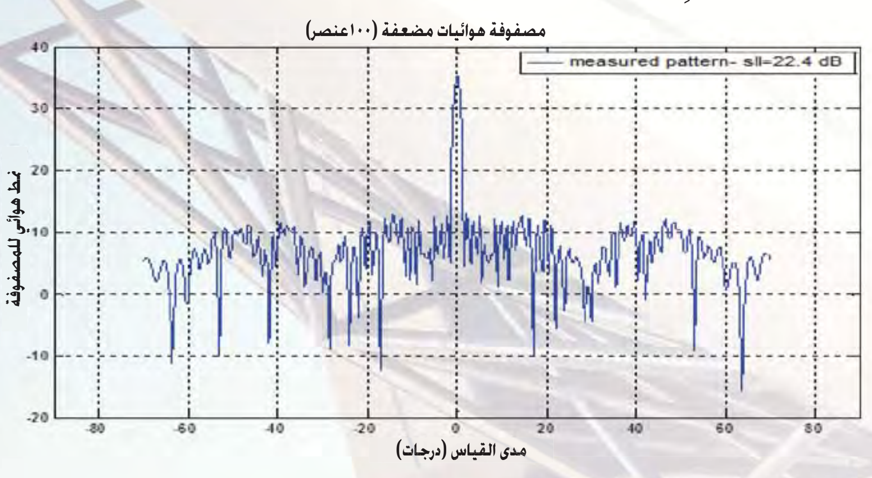
■ شكل (٧): مصفوفة هوائيّة مُضَعّفة منصوبة داخل غرفة كاتمة للصّدى



■ الغرفة كاتمة الصدى

النتيجة المُمَثَّلة ببرنامج الماتلاب. يوضِّح الشكل (٧) عيّنةً لمصفوفة هوائيّة وهي مُرَكَّبةٌ في غرفة القياس في المختبر - المُسمّاة غرفةً كاتمةً للصّدى (Anechoic Chamber) - وهي غُرْفَةٌ مُغلَقَةٌ بالكامل، ومُبَطّنة من الداخل بمادّة عديمة الارتداد؛ للسّماح للهوائيّ داخلَ الغرفة باستقبال الإشارة اللاسلكيّة مباشَرة من المَصْدَر دون أيّ إشارات دخيلة أخرى؛ ليُعْطِيَ دقّةً أكثرَ في قياس النّمط الهَوائيّ للهَوائيّ المنصوب داخلَ الغرفة.

قِيْسَ النّمط الهوائيّ لمصفوفة (١٠٠ عنصر) هوائيـاّت مُضعّفة خلال المدى (-70°:70°)، شكل (٨)، ويمكن ملاحظة أنّ قيمة مستوى الفلقة الجانبيّ مُنْخَفِضٌ (sll=−22.4 dB)؛ ممّا يعني قدرتَه على العمل بصورة مَرْضِيٌّ عنها في نظام رادار التتبّع أفضلَ من مصفوفة الهوائيّات المُتوافقة في الطّور.



■ شكل (٨) : النمط الهوائيّ لمصفوفة ١٠٠ عنصر هوائيّ مُضَعّفة

المراجــع

- Balanis, C. A. Antenna theory: analysis and design, 2nd ed. John Wiley & Sons, Inc., 1997.
- Barton, D. K. Radar System Analysis and Modeling. Artech House, 2005.
- du Plessis W. P. and A. bin Ghannam, “Sparse- and thinned-array literature survey and algorithm implementation,” CSIR, Pretoria, R.S.A., Report 5840-RATIP-00001 RPT Rev 2, 3 May 2012.
- Frank J. and J. D. Richards, “Phased array radar antennas,” in Radar Handbook, 3rd ed., M. I. Skolnik, Ed. McGraw-Hill, 2008, ch. 13.
- Haupt, R. L. “Thinned arrays using genetic algorithms,” IEEE Trans. Antennas Propag., vol. 42, no. 7, pp. 993–999, July 1994.
- Haupt, R. L.“Interleaved thinned linear arrays,” IEEE Trans. Antennas Propag., vol. 53, no. 9, pp. 2858–2864, September 2005.
- Hooker J. W. and R. K. Arora, “Optimal thinning levels in linear arrays,” IEEE Antennas Wirel. Propag. Lett., vol. 9, pp. 771–774, 2010.
- Hopperstad J. F. and S. Holm, “Optimization of sparse arrays by an improved simulated annealing algorithm,” in Proc. Int. Workshop on Sampling Theory and Applications, August 1999, pp. 91–95.
- Jin N. and Y. Rahmat-Samii, “Particle swarm optimization for antenna designs in engineering electromagnetics,” Journal of Artificial Evolution and Applications, vol. 2008, 2008.
- Keizer, W. P. M. N.“Linear array thinning using iterative FFT techniques,” IEEE Trans. Antennas Propag., vol. 56, no. 8, pp. 2757–2760, August 2008.
- Leeper, D. G. “Isophoric arrays – massively thinned phased arrays with well-controlled sidelobes,” IEEE Trans. Antennas Propag., vol. 47, no. 12, pp. 1825–1835, December 1999.
- Li, J. and P. Stoica, “MIMO radar – diversity means superiority,” in Adaptive Sensor Array Processing Workshop, June 2006.
- Li, J. and P. Stoica, “MIMO radar with colocated antennas,” IEEE Signal Process. Mag., vol. 24, no. 5, pp. 106 –114, Sept. 2007.
- Oliveri, G. M. Donelli, and A. Massa, “Linear array thinning exploiting almost difference sets,” IEEE Trans. Antennas Propag., vol. 57, no. 12, pp. 3800–3812, December 2009.
- Skolnik, M. I. J. W. Sherman, III, and F. C. Ogg, Jr, “Statistically designed density-tapered arrays,” IEEE Trans. Antennas Propag., vol. 12, no. 4, pp. 408–417, July 1964.

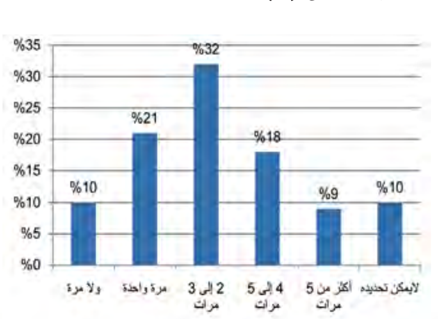
تشفير المعلومات

آلاء الطرباق - حنان الحليبة - مدى الحيدري



يتم تناقل المعلومات - في عصرنا الحاضر - بين المؤسسات والأفراد عبر الشبكات الإلكترونية المترابطة بكل يُسر وسهولة، ويشمل ذلك العمليّات الماليّة والحكومية. ونظراً لأنّ الشبكات الإلكترونية في الغالب تكون متوافرة للعامّة، فإن ذلك يجعل تلك المعلومات عرضة للسرقة والتزوير، ولتفادي ذلك لا بدّ من إجراء عمليّة تشفير لتلك المعلومات عن طريق إعادة ترميز البيانات باستخدام عمليات رياضية، لتصبح غير قابلة للقراءة من قِبل أيّ شخص غير مخوّل له صلاحية الاطّلاع على البيانات.

الجدير بالذكر أنّ استطلاعاً أجراه معهد بونيمون - شمل ٥٨٣ مختصًّا وممارسًا في تقنية المعلومات وأمنها - أظهر أنّ نسبة الهجمات الاختراقيّة الناجحة التي تعرّضت لها مؤسساتهم، بلغت ٥٩٪ (٣٢٪ + ١٨٪ + ٩٪) على الأقل لهجمتين ناجحتين خلال الـ ١٢ شهرًا الماضية، شكل (١).



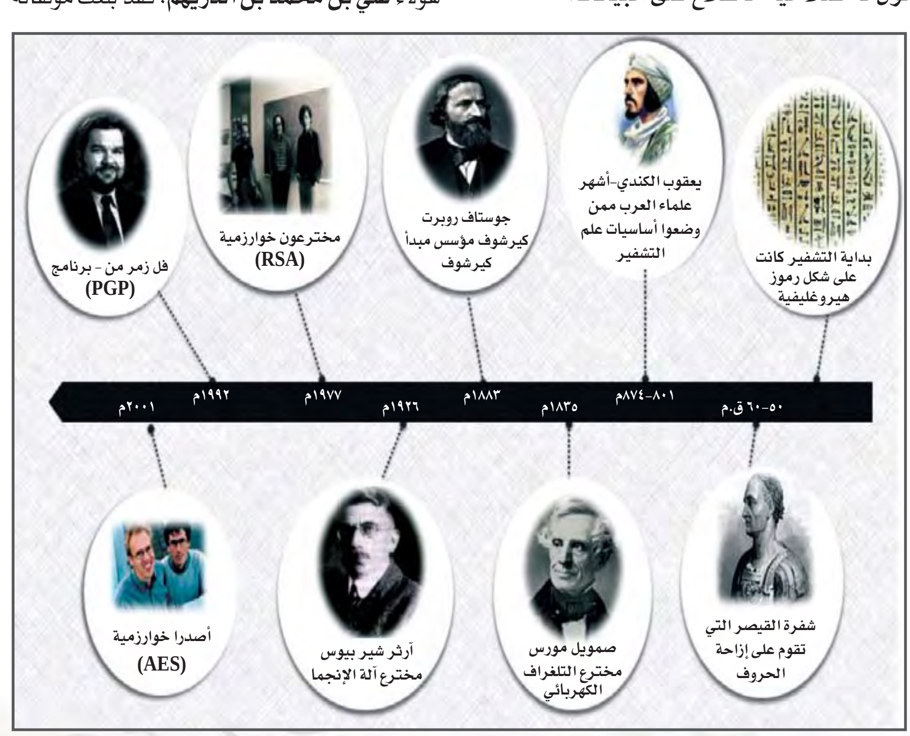
■ شكل (١) عدد المرّات التي تعرّضت فيها المؤسّسات التي شملها الاستطلاع لهجمات ناجحة.

التشفير في العهود القديمة

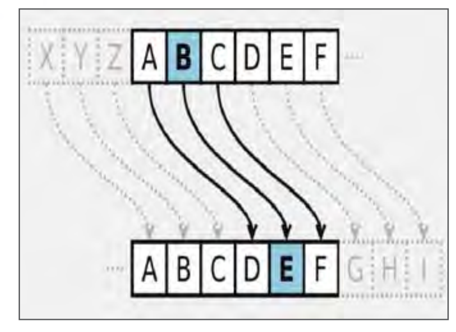
مرت عملية تشفير المعلومات بعدة مراحل منذ العهود القديمة حتى سبعينيات القرن الماضي، شكل (٢)، حيث كانت بدايات ظهور التشفير عند المصريين القدماء قبل ما يقارب ١٩٠٠ ق.م على شكل رموز هيروغليفية غير اعتيادية تم إدخالها في أماكن رموز أخرى - فيما عُرف بعملية الإبدال (Substitution) - لإعطاء طابع التفخيم والزخرفة على المعابد والآثار، ولم يكن الهدف منها إخفاء النص الأصلي.

بعد عدة قرون، قام الإغريق والرومان بمحاولات عديدة للتشفير تم استخدامها في مجال المراسلات الحربيّة، ولعلّ أبرزها كانت شفرة **يوليس قيصر** (٥٠ - ٦٠ ق.م)، شكل (٣) التي تقوم على إزاحة الحروف ثلاث خانات في سلسلة الأحرف الأبجديّة. فعلى سبيل المثال الحرف الأوّل يُستبدل بالحرف الرابع أبجديًّا وهكذا بالتسلسل. ونظرًا لكون أغلب أعداء قيصر أُميّين فقد نجحت تلك الشيفرة البسيطة وأثبتت فعاليّتها في ذلك العصر.

كان للعلماء العرب اليد العليا في وضع أسس علم التشفير ومبادئه، إذ لم يسبقهم إليها أحد، ومن أبرز هؤلاء **علي بن محمد بن الدريهم**. فقد بلغت مؤلّفاته



■ شكل (٢) التطور الزمني للتشفير.



■ شكل (٣) شفرة يوليوس قيصر.

في هذا المجال ٢١ مؤلفًا، مـن أشهرها «مفتاح الكنوز في إيضاح المرموز» الذي شرح فيه عمليّة فك التشفير، وأورد فيه مثالين عمليين في حلّ الترجمة، وقد قال عنهما **دافيد كهن** كبير مؤرخي التعمية في كتابه (The Codebreakers) إنّهما أوّل مثالين لفكّ التشفير في التاريخ.

كما اشتهر **أبو يوسف يعقوب بن إسحاق الكندي** (٨٠١-٨٧٤م) في هذا المجال بسبب ابتكاره طريقة فعّالة تعتمد على دراسة نسبة احتمال تكرار حرف ما حسب اللّغة ضمن النّص، وذلك باستخدام طُرُق إحصائيّة، واستغلالها في فكّ الشيفرات، كما هو مذكور في مخطوطته «مخطوط في فك رسائل التشفير».

في عام ١٨٣٥م اخترع **صمويل مورس** بمساعدة زميله **ألفريد** جهاز التلغراف الكهربائي، وهو جهاز يستخدم النبضات الكهربائية المختلفة المُرسلة عبر سلك معدنيٍّ من أجل التحكّم في المغناطيس الكهربائي الذي يوجد في النهاية المستقبلة من سلك التلغراف، لإنتاج رموز مكتوبة على شريط من الورق. تلا ذلك اختراع شيفرة **مورس** ١٨٤٤م التي تسمح بتحويل تلك الرموز المكتوبة إلى حروف وأرقام، حيث يتطلّب ذلك معرفة تامّة بالشيفرة ليتمكّن المستقبل من تحليلها / فكها.

أتى العالم الفيزيائي **غوستاف روبرت كيرشوف** في عام ١٨٨٣م بمبدأ **كيرشوف** (Kerckhoffs principle)، شكل (٤) الذي ينصّ على أنه: «يجب أن يكون نظام التشفير المستخدم آمنًا بالرغم من معرفة المهاجم بكلّ تفاصيل النظام باستثناء المفتاح السِّرّي. أي أنّه «ينبغي أن يكون النظام آمنًا رغم معرفة المهاجم بخوارزميّة التشفير وخوارزميّة فك التشفير» وهو المبدأ الذي يقوم عليه نظام التشفير في العصر الحديث، حيث إنّه من غير الملائم تصميم نظام تشفير جديد كليًّا في حال تسرُّب معلومات عن النظام، أو في حال الشكّ بمصداقيّته، فذلك يتطلّب استثمار جهد و وقت في كل مرّة، فاستبدال المفتاح يصبح أقل تكلفة وأسهل في حال وجود عدّة مستقبلين، فما على المُرسل فعله هو اختيار مفتاح مختلف لكلّ جهة مستقبِلة.

على سبيل المثال في حال أراد **أحمد** التواصل مع **بدر** فما عليه إلا استخدام مفتاح (Ks) لتشفير الرّسالة باستخدام خوارزميّة التشفير (E)، ومن ثم إرسال الرسالة المشفّرة عبر قناة غير آمنة، وعند استقبال **بدر** تلك الرسالة المشفّرة فإنه باستخدام المفتاح (Ks) وخوارزميّة فك التشفير (D) يمكنه استرجاع المحتوى الأصلي للرسالة.

في حال اطّلع المهاجم على الرسالة المشفّرة فلن يستطيع استرجاع المحتوى الأصلي، فهو لا يملك المفتاح المشترك (Ks) بين كلٍّ من **أحمد وبدر**.



■ شكل (٤) مبدأ كيرشوف.



■ شكل (٥) آلة إنجما المستخدمة في الحرب العالمية الثانية.

اخترع المهندس الألماني **آرثر شيربيوس** آلة «إنجما»، شكل (٥) متجاهلًا مبدأ **كيرشوف**، وتعني كلمة إنجما «لغز» باللغة الإنجليزيّة. وقد استخدم هذه الآلة الجيش الألماني عام ١٩٢٦م في الحرب العالمية الثانية، و كُسرت شيفرتها بعد اثنتي عشرة سنة من اختراعها قبل نهاية الحرب العالمية الثانية بخمسة أسابيع، وذلك نتيجة لتجاهله مبدأ **كيرشوف**. تكمن قوّة إنجما -كما افترض مصمِّمها- في طول المفتاح وسريّة تصميم الآلة. وتتألف إنجما من لوحة مفاتيح مكوّنة من ٢٦ حرفًا من اللغة الإنجليزية، ولوحة مصابيح، ولكل حرف مصباح، ومجموعة من دواليب دوّارة موصلة كهربائيًّا (كهروميكانيكية) تستخدم لإنتاج شيفرة سريَّة. فمع كل ضربة زر على لوحة المفاتيح يمرّ التيار الكهربائي من خلال هذه الدواليب مسبّبًا في إدارتها باتجاه عقارب الساعة حتى يصل التيار إلى لوحة المصابيح، مما يسبب إضاءة أحد تلك المفاتيح ومُنتجًا شيفرة مقابلة للحرف المُدخل.

التشفير في العصر الحديث

حتى عام ١٩٧٠م كانت جميع طُرُق التشفير حكرًا على الجهات الحكوميّة والأجهزة الأمنيّة فقط، لكن الأمر لم يدم طويلًا بعد اكتشاف أهم حدثين في عالم التشفير، وهما: خوارزميّات التشفير المتماثل (Symmetric-key cryptography) وخوارزميّات التشفير اللامتماثل، أي التشفير بالمفتاح العام (Public key cryptography):

● **التشفير المتماثل**

يعتمد التشفير المتماثل في الأساس على وجود مفتاح سريٍّ مشترك بين كلٍّ من المُرسل والمستقبل لكي يتمكّن كلٌّ منهما من تشفير وفكّ تشفير البيانات باستخدام المفتاح نفسه. يجري تنفيذ هذا النوع من التشفير على البيانات المُدخلة على أجزاء متساوية من النصّ (كتلة) ومن أشهر خوارزميّات التشفير المتماثل التي تعتمدها الحكومة الأمريكية للتشفير هي:

■ **معيار تشفير البيانات (Data Encryption Standard–DES)**: وهو عبارة عن خوارزميّة تشفير بمفتاح حجمه (٥٦ بت) لكلّ كتلة من البيانات بحجم (٦٤ بت)، وقد اعتمدت حكومة الولايات المتحدة الأمريكية هذا المعيار لأوّل مرّة في عام ١٩٧٧م، حيث كان عبارة عن مشروع ضمن مختبرات (IBM) يهدف إلى إنشاء خوارزميّة لا يمكن كسرها حتى باستخدام أسرع الأجهزة المتوافرة في ذلك الوقت. وقد وافق المعهد الأمريكي للمعايير القياسية (ANSI) على (DES) لكن أطلق اسم خوارزميّة تشفير المعلومات (Data Encryption Algorithm –DEA) عليها عوضًا عن (DES).

على الرغم من أنها لم تُصنّف كمقياس رسمي، إلا أنّ معيار تشفير البيانات (DES) هو أكثر طُرُق التشفير شعبيّة (خصوصًا مقياس تشفير البيانات الثلاثي الذي يُستخدم في كثير من التطبيقات، مثل: تشفير أجهزة الصرّاف الآلي، والبريد الإلكتروني، ومن أكثر من يلجأ إلى استخدام التشفير الثلاثي باستخدام (DES) هو المؤسّسات والمعاهد الماليّة التي نصّبت معدّات (DES) سابقًا لديها.

بغض النظر عن جميع ما ذُكر فإنّ تبني طريقة التشفير الثلاثي باستخدام (DES) ضمن البرمجيّات يُعدُّ بطيئًا بالمقارنة مع الـ (DEA) حيث يجب أن يتم تطبيق توابع الـ (DES) ثلاث مرّات، بالإضافة إلى أن التشفير الثلاثي باستخدام (DES) يستخدم الحجم نفسه لما يُدعى (Block size) وهو ٦٤ بت كما هو الحال في ال (DES) الذي يُعدُّ ضعيفًا. تم كسر هذا التشفير في عام ٢٠٠٨م واستبداله بمعيار التشفير المتقدّم في أغلب الاستخدامات.

■ **معيار التشفير المتقدّم (Advance Encryption Standard-AES)**:

وهو عبارة عن معيار أعلن عنه المركز القومي للمعايير والتكنولوجيا فرع حكومة الولايات المتحدة (NIST) في مسابقة لتطوير مقياس تشفير متطور (AES) بديل لـ (DES) وذلك لأنها كانت تُعدُّ آنذاك غير آمنة بسبب تطوير وسائل متطوّرة لكسر هذه الوسيلة، وعليه يجب أن تحقق هذه الخوارزميّة الجديدة مجموعة من المعايير التي وضعها المعهد، وهي: أن تكون خوارزميّة مفتوحة للعوام، ومتوافرة بشكل مجاني للجميع حول العالم. تم ترشيح ١٥ بحثًا للمشاركة في المؤتمر الأول لمرشحي المعايير القياسيّة للتشفير المتقدّم (The First Candidate Conference -AES1)، حيث اختار المعهد– فيما بعد– خمس خوارزميّات من أصل الـ ١٥ خوارزميّة المشاركة هي (Serpent, Rijndael, RC6, Marcs, Twofish). وجَرَت مراجعتها بشكل أكبر ضمن فترة من الزمن للتوصل إلى الاختيار النهائي.

في عام ٢٠٠٠م أعلن المعهد عن اختياره خوارزميّة (Rijndael) «ران دول» لتُعتمد في عملية التشفير المتقدمة (AES) التي ابتكرها عالما تشفير من بلجيكا، هما: **جون دايمين وفنسنت ريجمين**.

تتميّز خوارزمية الـ (AES) بصعوبة كسرها والعثور على المفتاح، وذلك بسبب طول المفتاح المستخدم في التشفير، لذلك تُعدُّ طريقة آمنة للتشفير. وتوفر (AES) ثلاث خيارات لطول المفتاح، وهي كالآتي: ١٢٨، ١٩٢، أو ٢٥٦ بت. كذلك تتميز هذه الخوارزميّة بكبر حجم الكتلة (Block size) الذي يساوي ١٢٨ بت.

الجدير بالذكر أن خوارزميّة الـ (AES) لها كثير من الاستخدامات التي تضمن حماية المستخدم عبر الإنترنت لتصل إلى حماية وضمان البيانات في البنوك والمعامل، كما أنّ لها استخدامات في المجالات العسكريّة. ومن أشهر البرامج والبروتوكولات التي تعتمد على مقاومة (AES) للهجمات الإلكترونية:

١- برامج (WINZIP) في حالة أنّ المُستخدم طلب تشفير البيانات بعد ضغطها.

٢- بروتوكول (TLS) وهو بروتوكول لإنشاء اتصال آمن.

٣- بروتوكول (IPsec) وهو بروتوكول لضمان الأمان في الاتصالات التي تعمل بوساطة (IP) عبر الإنترنت.

■ **خوارزمية تشفير البيانات الدولية (IDEA):**

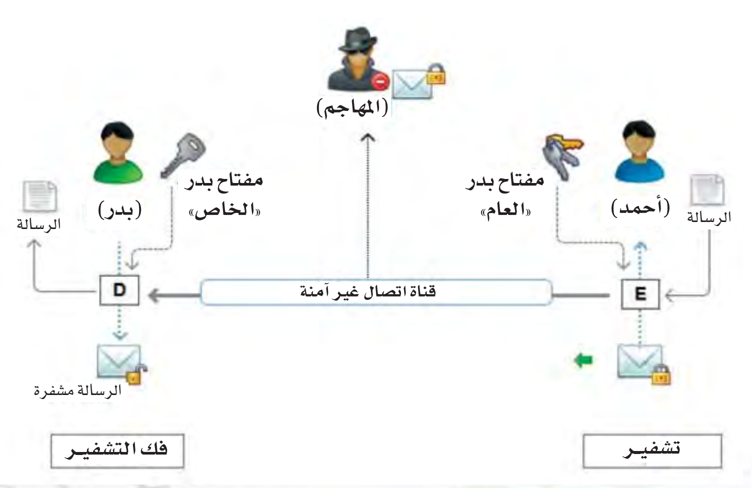
وهي إحدى خوارزميّات التشفير المتماثل الآمنة. طوّر هذه الخوارزمية المعهد الفدرالي للتكنولوجيا بزيورخ، سويسرا، و تتميز هذه الخوارزمية بكبر حجم الكتلة (Block size) الذي يساوي ١٢٨ بت.

من الجدير بالذكر أن (IDEA) هو عبارة عن براءة اختراع لصالح أسكوم للتكنولوجيا ومحفوظة في كلٍّ من الولايات المتحدة ومعظم الدول الأوروبية، وقد انتهت صلاحية براءة الاختراع هذه في عام ٢٠١٢م وهو الآن متاح بالمجان لأي شخص دون قيود.

■ **CAST**: وهو أحد أنواع التشفير المتناظر. ابتكره عالما تشفير، وهما: **كارلايل أدامز وستافورد تافاريس** في عام ١٩٩٦م. توفر (CAST) إمكانية لاختيار حجم المفتاح ابتداءً من ٤٠ إلى ١٢٨، مع ثبات الكتلة عند ٦٤ بت. وافقت الحكومة الكندية على استخدام هذه الخوارزميّة، وتحديدًا من قبل مؤسسة أمن الاتصالات.

● **التشفير بالمفتاح العام**

يستخدم التشفير بالمفتاح العام (Public Key Cryptography)، شكل (٦)



■ شكل (٦) التشفير باستخدام المفتاح العام.

زوجًا من المفاتيح مرتبطًا بعلاقة عوضًا عن استخدام مفتاح مشترك. وهما:

١- مفتاح عام (Public key) وهو معلن للجميع، ويستخدم من قِبل المُرسل لتشفير الرسالة للمستقبل.

٢- مفتاح خاص (Private key) ويكون في طي الكتمان، يملكه المستقبِل لفك تشفير الرسائل المرسلة إليه، ولا يمكن فك التشفير إلا باستخدامه.

الجدير بالذكر أنّ فكرة المفتاح العام بدأت كوسيلة لحل مشكلة توزيع المفاتيح في التشفير المتماثل، ففي التشفير المتماثل يحتاج كلا الطرفين إلى مفتاح مشترك مستقلّ بينهما، فإن أراد الشخص التواصل مع خمسة أشخاص مختلفين فذلك يعني الاحتفاظ بخمسة مفاتيح مختلفة، وتزداد المشكلة حجمًا بازدياد عدد الأشخاص المرغوب في التواصل معهم، وليس ذلك فحسب فتلك المفاتيح تحتاج إلى تبادل مسبق من خلال اللّقاء الشخصي، أو من خلال قناة آمنة قبل القيام بعملية التشفير.

يعتمد التشفير بالمفتاح العام في كثير من عملياته على نظريّة الأعداد (Number theory)، وهو فرع من فروع علم الرياضيات مهتمّ بدراسة الأعداد الصحيحة، و خصائصها، والعمليّات التي تجري عليها.

تنصّ نظريّة الأعداد على أنّ الأعداد تنقسم إلى: أعداد أوليّة وأعداد مؤلّفة. فالأعداد الأوليّة هي الأعداد التي تقبل القسمة على واحد ونفسها فقط، أمّا الأعداد المؤلّفة فهي الأعداد التي لها أكثر من قاسمين، وقد سمّيت بمؤلفة لأنها مركّبة من جداء الأعداد الأوليّة، أي أنّ الأعداد الأوليّة هي أساس أي عدد صحيح. فعند تحليل العدد ٤٥ إلى عوامله الأوليّة (بـ القسمة المتتابعة على الأعداد الأوليّة) نحصل على ٥×٣^٢.

كما يمكن القول إنّ العددين (أ) و (ب) أوليّين فيما بينهما (Relatively prime) في حال لم يوجد عامل مشترك بينهما غير الواحد، ويمكن العثور على العامل المشترك بين عددين بشكل أسرع من تحليلهما إلى عواملها الأولية وذلك باستخدام خوارزميّة **أقليدس** (Euclidean Algorithm) التي تنص على أنّ القاسم المشترك الأكبر لعددين طبيعيّين (أ)، (ب) يساوي القاسم المشترك الأكبر للعدد الثاني (ب) وباقي قسمة (أ) على (ب)، ويمكن تكرار العمليّة نفسها حتى يصبح باقي القسمة مساويًا الصفر، عندئذ يكون القاسم المشترك الأكبر هو العدد الآخر.

فعلى سبيل المثال لنفرض أنّنا أردنا العثور على العامل المشترك بين ١٢٣ و١٢ وتكتب gcd (123,12).

فعلينا فعل الآتي:

- نقسم ١٢٣ على ١٢ (العدد الأكبر على الأصغر)، فسيكون ناتج القسمة ١٠ والباقي ٣.

- نقسم ١٢ على ٣ فسيكون الناتج ٤ والباقي صفر، إذًا القاسم المشترك الأكبر هو ٣.

ويمكن الحصول على باقي القسمة من خلال الحسابات النمطيّة (Modular arithmetic) وهو نظام حسابي للأعداد الصحيحة يركّز على دراسة باقي حاصل القسمة حول عامل ما (Modulus) و تُكتب العملية كالآتي:

9 mod2 =1 أي باقي قسمة ٩ على ٢ يساوي ١.

من أشهر خوارزميّات التشفير بالمفتاح العام ما يلي:-

■ **خوارزمية ديفي هيلمان لتبادل المفاتيح:** وهي عبارة عن مخطّط مبدئيّ لتبادل المفاتيح تم نشرها عام ١٩٧٦م بوساطة الزميلين: **وايتفيلد ديفي و مارن هيلمن** في ورقة بحثية بعنوان «الاتجاهات الجديدة في التشفير – New Directions in Cryptography» حيث أوضحا طريقة تسمح لطرفين لم يسبق لهما اللقاء بتكوين مفتاح مشترك عبر قناة اتصال غير آمنة.

يمكن شرح الطريقة بشكل مبسط كالآتي:

- يتفق **أحمد وبدر** على جذر أولي (g) وعدد أولي (p) بشكل علني.

- يختار **أحمد** رقمًا طبيعيًّا عشوائيًّا (a) ثم يرفع (g^a)، يحتفظ **أحمد** بـ (a) ويرسل (g^a) إلى **بدر**.

- يختار **بدر** رقمًا طبيعيًّا عشوائيًّا (b) ثم يرفع (g^b)، يحتفظ بدر بـ (b) ويرسل (g^b) إلى **أحمد**.

- يحسب **أحمد** $(g^b)^a \bmod p$ ويحسب **بدر** $(g^a)^b \bmod p$ وهو المفتاح المشترك بينهما.

مما يجدر ذكره أنّ الزميلين عرضا فكرة التشفير باستخدام المفتاح العام، لكنّهما لم يقدّما تطبيقًا عمليًّا على ذلك، بعد سنة من نشر مقالهما عام ١٩٧٧م ظهرت خوارزميّة (RSA) بالتطبيق العمليّ.

■ **خوارزمية آر إس ايه (RSA):** وتعدُّ أحد أشهر خوارزميات التشفير بالمفتاح العام والتي تأخذ حروفها من أسماء مخترعيها **رون ريفيست وَأدي شامير وَليونارد أدليمان** ويقوم مبدأ عملها على الصعوبة الإفتراضية لتحليل الأعداد الصحيحة الكبيرة إلى عواملها الأولية.

تقوم خطوات توليد مفتاح (RSA) بشكل مختصر كالتالي:

- يقوم **بدر** باختيار عددين أوليين عشوائيّين (p) ,(q) وحساب $n = p.q$

- يختار **بدر** عدد صحيح (e) حيث:

$$gcd\,[e,(p-1)(q-1)] \equiv 1$$

ثم يقوم بإيجاد (d) بحيث يحقق التالي:

$$e.d \equiv 1$$

- يقوم **بدر** بالإعلان عن (n) و (e)، ويحتفظ بـ (p, q, d) في طي الكتمان.

فإن أراد **أحمد** التواصل لإرسال رسالة (M) **لبدر** فعليه استخدام المفتاح العمومي المعلن لبدر (n, e) وذلك بتطبيق معادلة التشفير:

$$C=M^e \pmod n$$

ثم يرسل النص المشفر (C) إلى **بدر**.

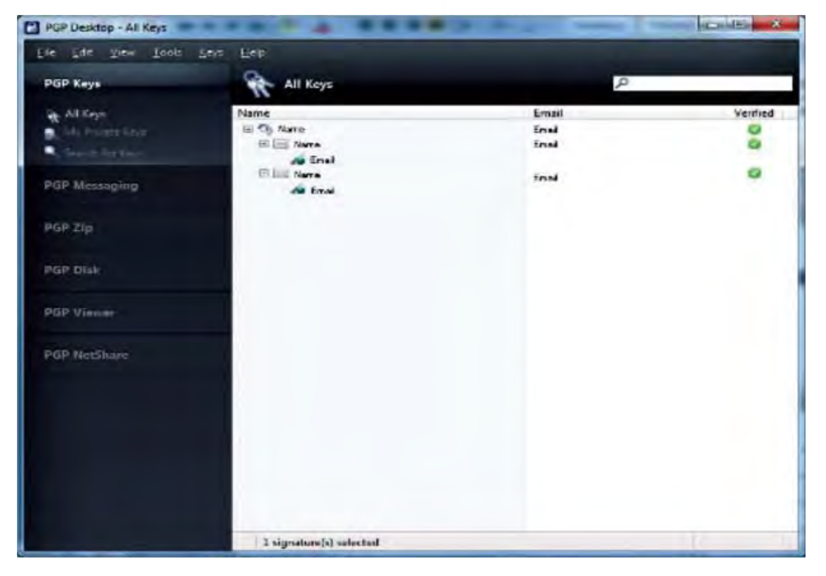
يقوم **بدر** باستلام النص المشفر (C) ويستخدم مفتاحه السري (d) لفك التشفير من خلال معادلة فك التشفير للحصول على الرسالة المرسلة (M):

$$M=C^d \pmod n$$

● خصوصية جيد جداً

يعد برنامج خصوصية جيدة جداً (Pretty Good Privacy-PGP) من أشهر البرامج المستخدمة في عصرنا اليوم لتشفير الملفات والمعلومات، وهو من تصميم **فل زمير من** والذي تم إصدار أول نسخة منه عام ١٩٩٢م، شكل (٧).

من الجدير بالذكر أن (PGP) لايطلق فقط على البرنامج وإنما أيضا على البروتوكول المستخدم لهذا النظام. يهدف هذا النظام لتشفير محتويات البريد الإلكتروني لضمان سريتها وسلامتها وللتأكد من هوية المرسل. ولتحقيق هذا النوع من الاتصال الآمن جمع



■ شكل (٧) واجهة برنامج خصوصية جيدة جدا.

هذا النظام أفضل خوارزميات التشفير المتاحة من كلا من خوارزميات التشفير المتماثل وغير المتماثل، وخوارزميات الهاش والتوقيع الرقمي.

يعمل الـ (PGP): حسب الخطوات التالية:

١- عند رغبة المستخدم بتشفير النص يقوم البرنامج أولا بضغط البيانات و تتم هذه العملية من خلال الاستفاده من تكرار الأحرف أو الرموز داخل هذه البيانات مع الأخذ بعين الاعتبار إمكانية استرجاع هذه البيانات. تهدف عملية ضغط البيانات إلى تقليل حجمها لتوفير مساحة الذاكرة، والتخفيف من حركة مرور البيانات عبر الشبكة، وأيضاً إحباط وتقليل نسبة الهجمات وذلك نظراً لأن أغلب عمليات الهجوم تتم باستغلال تكرار الأحرف.

٢- إنشاء البرنامج لمفتاح سري يستخدم لمرة واحدة فقط لتشفير النص الحالي. ويتم انشاء المفتاح السري بشكل عشوائي بالاستعانة بمواقع حركة المؤشر ولوحة المفاتيح.

٣- تشفير النص باستخدام المفتاح المنشأ مع إحدى خوارزميات التشفير المتماثل.

٤- تشفير المفتاح السري السابق باستخدام المفتاح العام للمستقبل.

٥- إرسال النص والمفتاح السري المشفر للاطراف المعنية.

٦- فك التشفير بشكل عكسي، حيث يقوم البرنامج بفك المفتاح السري المشفرعن طريق استخدام المفتاح الخاص للمستقبل. بعد فك تشفير المفتاح واستخراجه يستخدم هو بالتالي لفك تشفير النص.

ويلاحظ مما سبق أن تشفير النص يتم باستخدام إحدى خوارزميات التشفير المتماثل وذلك نظراً ماتتميز به بقدرتها على تشفير البيانات بشكل أسرع وبكميات أكبر على نقيض خوارزميات التشفير اللامتماثل. لكن تلك الأخرى تتميز بقوة مفاتيحها وصعوبة كسرها، لذلك تستخدم هي بالتالي في تشفير المفاتيح.

■ **أنواع الـ (PGP):** وهما نوعان:-

- **النوع الأول:** ويدعم خوارزمية الـ (RSA) الذي يتطلب من المستخدم دفع رسوم لمنظمة الـ (RSA). في هذا النوع يتم استخدام خوارزمية (IDEA) لتوليد المفاتيح وتشفير البيانات ومن ثم استخدام خوارزمية الـ (RSA) لتشفير المفاتيح المولدة من قبل (IDEA). وفي حالة الرغبة لتوثيق هوية المرسل يتم ارسال التوقيع الرقمي للمرسل والذي يتم حسابه عن طريق خوارزمية MD5 (إحدى خوارزميات الهاش).

- **النوع الثاني:** ويدعم خوارزمية (Diffie-Hellman) وفيه يتم استخدام خوارزمية (CAST) لتوليد المفاتيح وتشفير البيانات ومن ثم استخدام خوارزمية الـ (Diffie-Hellman) لتشفير المفاتيح المولدة من قِبل (IDEA). وفي حالة الرغبة لتوثيق هوية المرسل يتم ارسال التوقيع الرقمي للمرسل الذي يتم حسابه عن طريق خوارزمية (SHA-1) وهي إحدى خوارزميات الهاش.

■ **OpenPGP:** وهو معيار وضع بناءا على (PGP) الذي أنشئ من قبل **فل زمرمن**. تم وضع وتحديد هذا المعيار من قبل فريق مهام هندسة الإنترنت (IETF) في عام ١٩٩٧م. ويوضح هذا المعيار كيفية بناء برنامج مكافئ (PGP) لتشفير البريد الإلكتروني باستخدام إحدى خوارزميات التشفير اللامتماثل.

المراجع

- كتاب علم التعمية واستخراج المعمى عند العرب – الجزء الأول مجمع اللغة العربية ، دمشق ، ١٩٨٧ ، تقديم أ.د.شاكر الفحام.
-Example of Caesar method, http://upload.wikimedia.org/wikipedia/commons/2/2b/Caesar3.svg.
-Introduction to cryptography and Network security by Behrouz A. Forouzan, April 1, 2007.
-Perceptions About Network Security: Survey of IT & IT security practitioners in the U.S, June 2011.
-The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet by David Kahn, December 5, 1996.
-Three-ring Enigma cypher machine in wooden transit case, c 1930s.
-Understanding Cryptography by Christof Paar Jan Pelzl, Jul 8, 2010.
-http://www.juniper.net/us/en/local/pdf/additional-resources/ponemon-perceptions-network-security.pdf.
-http://www.sciencemuseum.org.uk/images/I036/10305537.aspx
-http://searchsecurity.techtarget.com/definition/International-Data-Encryption-Algorithm
-http://en.wikipedia.org/wiki/CAST-128
-http://www.haladeeb.name/2008/08/18/cryptographic-techniques-1/
-http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
-http://www.cs.cornell.edu/courses/cs5430/2010sp/TL03.symmetric.html
-http://www.federica.unina.it/ingegneria/security-and-dependability-of-computer-systems/network-security/
-https://web.cs.dal.ca/~tt/ECMM6010/presentations/PGP.pdf
-http://www.openpgp.org/about_openpgp/
Introduction to Cryptography with Coding Theory, 2nd edition

أجهزة التشفير .. هل تحمينا؟

م/ صلاح بن سعد الطّخيس

تُعَدّ المحافظة على سرّيّة البيانات وضمان عدم العبث بها أساسَ علم أمن المعلومات، وبتطبيق هاتين الخاصيّتين يضمن الفردُ والمؤسّسة الأمان لتعاملاتهم اليوميّة؛ إذ يعتقد بعضهم أنّه باقتنائه أحدثَ جهاز تشفير وأقْواه يكفي لحماية معلوماته الحسّاسة، سواءٌ أكانت شخصية أم خاصّة بالشركة أم معلومات تُهمُّ أمن الدَّوْلة. وتعتمد هذه الأجهزة على ما يُسَمّى عمليّات التشفير، وهي سلسلة من العمليّات الرّياضيّة المعقّدة (خوارزميات) باستخدام مفتاح للتّشفير؛ إذ أن تغيّر محتوى نصّ (بيانات) إلى رموز وأرقام يصعب فَهْمُها. ومن أشهر هذه الخوارزميّات: خوارزميّة معيار التّشفير المتقدّم (Advanced Encryption Standard- AES) وخوارزميّة الـ(Rivest Shamir and Adleman- RSA) نسبة إلى العلماء الثلاثة الذين ابتكروها. تستمدّ هذه الخوارزميات قوّتها من صعوبة فكّ العمليّات الرّياضيّة المُسْتَخْدَمة، وأيضًا حجم مفاتيح التّشفير الممكن استخدامها، ومثال ذلك أنه ليست كلّ الأجهزة تدعم خوارزميّة الـ(AES) مع مفتاح حجمُه ٥١٢، ونظرًا إلى قوّة هذه الخوارزميّات لم يستطع علماء فكّ الشفرات (Cryptanalysis) فكّها وإيجاد ثغرات عمليّة أو تطبيقيّة عليها.



لكنّ مع التطوّر الكبير للتّقنية ظهرت في الآونة الأخيرة تهديداتٌ وهَجَمات فيزيائيّة جديدة ومُستَحدَثة على مثل هذه الأجهزة، تركّزت في اكتشاف الثّغَرات في الأجزاء الصُّلبة للحاسب (Hardware)، وعلى تحليل الإشعاعات المُنبعثة من هذه الأجهزة، وتحليل الطاقة الكهربائيّة باستخدام أجهزة متطوّرة للقيام بهذه الاختبارات والتحليل؛ فعند نجاح مثل هذه الهَجَمات يستطيع المخترِق معرفة مفاتيح التّشفير المستخدَمة في الجهاز، وبعد ذلك فكّ تشفير (Decrypt) المعلومات المشفَّرة سواءٌ أكانت مخزَّنة أم مُرْسَلة؛ مما يشكِّل تهديدًا صريحًا واختراقًا أمنيًّا يمكن أن يؤدّيَ إلى ما لا يُحْمَد عقباه.

يتناول هذا المقال مكوّنات أجهزة التّشفير، وبعض أهمّ الهَجَمات، وطرق الوقاية والحماية منها.

أنواع أجهزة التّشفير

تُقَسَم أجهزة التشفير إلى نوعَيْن، هما:

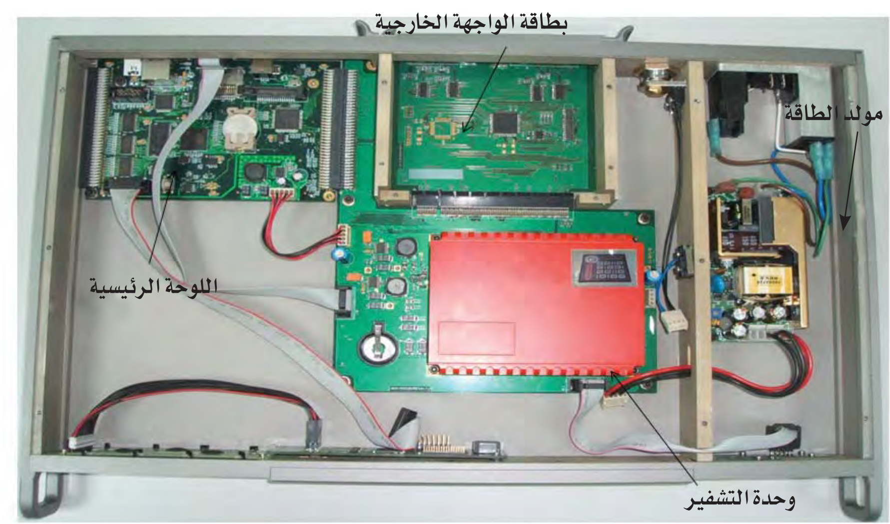
- أجهزة تشفير ونُظُم كبيرة إلى حدٍّ ما، وتُستخدَم في تشفير الشبكات الشّخصيّة الافتراضية (Virtual Private Line – VPN)، وتشفير القرص الصُّلْب، وتشفير وحدات التخزين الخارجيّة (Flash Memory) وغيرها.
- البطاقات الذكيّة وبطاقات الدّخول وما تحتويها من معلومات حسّاسة، مثل: معلومات الشّخص، والأرقام السّريّة، وغيرها.

مكوّنات أجهزة التّشفير

يتكوّن جهاز التشفير -عادة- من مكوِّنات و وحدات مختلفة؛ إذ إنّ لكلّ وحدة وظيفَتها الخاصّة والمحدَّدة في الجهاز؛ بحيث تتكامل هذه المُهِمَّات مع بعضها بعضًا؛ ليتشكّل جهاز تشفير متكامل، وهنالك عدّة تصاميم داخليّة لمثل هذه الأجهزة، ولكنّ أغلبَها يحتوي الوحدات الأساسيّة، شكل (١)، الآتية:

- **وحدة التشفير**

تُعَدّ وحدة التّشفير (Crypto Modules) عَصبَ الجهاز والمسؤولة عن عمليّات التشفير (Encryption) وفكّ التشفير (Decryption) جميعها، وإدارة المفاتيح، والعمليّات الأخرى المتعلقة بالتشفير كلّها، مثل التّصديق الإلكتروني، أو إنشاء مفاتيح سرّيّة جديدة. قد تتكوّن وحدة التشفير من معالج صغير (Microprocessor) يعتمد نوعُه على حجم جهاز التشفير ووظيفته ونوعه، ويحتوي في الغالب ذاكرة عشوائيّة



■ شكل (١) مكونات جهاز تشفير.

(Random Access Memory-RAM) وذاكرة دائمة خاصّة للتخزين.

● **اللوحة الرئيسية**

تمثّل اللوحة الرئيسيّة (Main Board) أداة التحكّم الرئيسة للجهاز، والمسؤولة عن التحكّم والرّبط بين الوحدات الداخليّة، كما تُستَخدَم لدعم وحدة التشفير وحملها.

● **بطاقة الواجهة الخارجيّة**

تُعَدّ بطاقة الواجهة الخارجيّة (External Interface card) المسؤولَة عن تحويل جميع البيانات المرسَلة من الجهاز وإليه حسب واجهته؛ فمثلًا في جهاز تشفير الهاتف تحوِّل البطاقة البيانات الرّقمية إلى إشارات تناظريّة (Analog Signals)، وتُرْسِلُها عن طريق شبكة الهاتف والعكس صحيح من تحويل الإشارات التناظرية الداخلة للجهاز إلى بيانات رقمية مفهومة للوحدات الداخلية للجهاز.

● **وحدة البطاريّة**

تمدّ وحدة البطاريّة (Power Supply) الجهاز بالطاقة، سواء أكانت بطاريّات متنقّلة وخفيفة أم وحدة موصولة مباشرة بتيّار كهربائيّ.

● **وحدة نقل البيانات وخطوط التحكّم الداخلية.**

ممّا سبق ذكره يتّضح أنّ وحدة التشفير تحتاج إلى تصميمٍ خاصّ؛ بحيث يضمن عدم وجود أيّ ثغرات أمنيّة فيها، كما أنّها تحتاج إلى عناية فائقة؛ لاحتوائها مفاتيح التشفير والبيانات الحسّاسة للنظام جميعها؛ فإذا تعرّضت هذه الوحدة للتهديد أو اُخْتُرِقَت دفاعاتها ، فهذا يعني تعرّض كلّ جهاز التشفير للاختراق، ويجب تصرّف المختصّ؛ إمّا بإعادة الجهاز إلى وضعه المصنعيّ أو التخلّص منه.

التهديدات والهجمات على أجهزة التشفير

تختلف الهَجَماتُ على أجهزة التشفير عن غيرها من الهجمات؛ إذ إنها لا تتمّ بالطّرق التقليديّة من انتشار فيروسات أو برامج خبيثة أو هجمات حاسوبية أخرى، بل تقصد إلى معرفة المعلومات السّريّة الموجودة في أجهزة التشفير واكتشافها، بأيّ طريقة ممكنة. وتنقسم هذه الهجمات إلى ثلاثة أنواع، وهي:

● **الهجمات الفيزيائيّة والتخريبيَة**

تغيّر الهَجَمات الفيزيائيّة والتخريبيّة (Physical & Invasive Attacks) من حالة النظام وتصرّفه، ويبقي أثرها في جهاز التّشفير دليلًا على حدوثها. تقصد هذه الهَجَمات بصفة أساسيّة إلى معرفة تامّة بتخطيط الوحدات الدّاخلية ووظائفها؛ لاستخلاص المعلومات الحسّاسة، ويحتاج هذا النوع من الهجوم إلى أجهزةٍ مرتفعةِ الثّمن، وتجهيزاتٍ خاصّة، ومهارة تقنية عالية؛ لتنفيذها، وتأتي تلك الهجمات على مرحلتين، هما:

١- الوصول المباشر إلى الوحدات الدّاخلية للجهاز؛ إذ يُفتَح فيها الجهاز؛ إمّا بنزع كلّي أوجزئيّ للغطاء (Decapsulation)، أو باستخدام موادَّ كيميائيّة دقيقة (Chemical Etching)؛ لتمويع الغطاء، وفصل الأجزاء عن بعضها بعضًا، ويجب أن تكون دقيقةً جدًا، ولا تُسَبّب عطلًا وتلفًا للوحدات الدّاخليّة.

٢- الهندسة العَكْسيّة (Reverse Engineering) والتّحليل العميق؛ لتصميم الوحدات الداخلية، ومعرفة كلّ الدوائر الإلكترونية والترانزتورز (Transistors) ومواقعها على الوحدات، وأيضًا الموصلات الداخلية بينها. ويتمّ ذلك عن طريق: التّصوير المرئيّ الدقيق للوحدات باستخدام جهاز عالي الدقّة (Micro Probing)؛ إمّا لمراقبة نقل البيانات بين الوحدات واكتشاف مفاتيح التشفير، أو إدخال إشارات معيّنة لوحدة التشفير؛ حتّى يبوح بمكنوناته السّرية.

● **الهجمات غير التخريبيّة**

الهجمات غير التخريبيّة (Non-Invasive Attacks) هي هجماتٌ تحليليّة لمُخْرَجات الجهاز المختلفة، دون الوصول المباشر للجهاز، ولا يكون لها أيّ أثر في الجهاز المراد اختراقه؛ لأنّها إشارات تحليليّة، وبعد تحليل هذه المُخرَجات يستطيع المخترق استنتاجَ المفاتيح السّريّة؛ وتُعَدّ هذه أخطر الهجمات؛ لعدم معرفة تعرّض الجهاز للهجوم. وبصورة عامّة تُعَدّ الهجمات غير التخريبيّة خطرة جدًا؛ ولذلك فقد ازدادت الأبحاث في هذا المجال، خصوصًا أنّ الأجهزة المطلوبة ليست مرتفعة السّعر، ولكنّ تحليل مثل هذه الهَجَمات يتطلّب وقتًا طويلًا.

تَنْقسم الهجمات غير التخريبيّة إلى نوعين، هما:

■ **هجوم خامل (Side Channel Attacks):**

ويتمّ بتحليل الإشارات الإلكترومغناطيسيّة المُنبثِقة من الجهاز، دون أيّ تدخل من المُهاجم (كلّ جهاز إلكتروني يرسل إشعاعاتٍ عفويّةً وغير

مقصودة) سواء عن طريق سلك الطّاقة أم من الجهاز نفسه، أم من شاشة الجهاز إن وجدت، ولذلك تبرز الحاجة إلى استخدام جهازٍ لقياس قوّة الإشارة (Oscilloscope)؛ لعمل مثل هذه الهجمات التي تنقسم إلى ثلاثة أنواع، هي:

- **هجوم بالتّحليل الوقتيّ (Timing Attacks):** إذ يُحْتَسَب الوقت لكلّ عمليّة، وبناء على أنماط معيَّنة، ومع كمّيّة كبيرة من البيانات المرسَلة يستطيع المهاجم معرفة نوع خوارزمية التشفير، ومن ثَمّ معرفة المفاتيح المستخدمة أو الأرقام السّريّة المُدخَلة؛ إذ وُجِدَتْ كثير من خوارزميّات التّشفير عرضةً لهذا الهجوم.

- **هجوم كاسح (Brute Force Attacks):** ويتمّ بتجربة جميع التركيبات المنطقية المكنة كمدخلات للجهاز، ومراقبة المخرَجات جميعها وتحليلها، واستنتاج نوع الخوارزمية، وأماكن الأخطاء (Fault)، ويُسَمَّى أيضًا اختبارَ الصّندوق الأسود.

- **تحليل الطاقة (Power Analysis):** ويُعَدّ من أقوى أنواع الهجوم، ونجح في اكتشاف مفاتيح تشفير لعدّة خوارزميات مُعْتَمَدَة، ومنها خوارزميّة (AES) عند استخدامها في معالجَات صغيرة، ويتمّ هذا الهجوم بتحليل استهلاك الطاقة الخارجة من الجهاز لكلّ عملية أمنيّة حسّاسة أو مرتبطة بالتشفير وقياسها؛ بحيث تُصَفّى الإشارة أولًا ومن ثَمّ تُحلّل لاكتشاف بت (bit) واحد ذي أهميّة في جدولة المفتاح في خوارزميات التشفير (key scheduling in cryptographic algorithms)، ومع تجميع كميّة كافية من البيانات وتحليلها، وبمعرفته المُسَبَّقة بنوع الخوارزمية؛ يعمل المهاجم موازنة بين النتائج؛ إذ يستطيع اكتشاف مفتاح التشفير. وهناك نوعان من هذا الهجوم، هما: تحليل الطّاقة اليسير (Single Power Analysis –SPA) وتحليل الطاقة الاختلافي (Differential Power Analysis-DPA).

■ **الهجوم النَّشط (Active Attacks):** ويستخدم استراتيجية الهجوم الخامل في التحليل نفسها، إلّا أنّه يتمّ بإرسال إشارة بطريقة معيَّنة، أو وضع الجهاز بحالة غير طبيعيّة، وتحليل المخرَجات من الجهاز، وتكون هناك تغيّرات واضحة على الجهاز، تتمثّل في نوعين، هما:

- **الهجوم الصّاعق السّريع (Glitching Attacks):** وهو تغيّرات سريعة جدًا في الإشارات الدّاخلة إلى الجهاز برمجها مخرّبون؛ لجعل الجهاز يخرج عن المألوف، ولا ينفّذ وظائفه الأمنيّة بطريقة مناسبة، وأقواها وأسهلها هجوم التّوقيت (Clock Glitching)، عندما يكون المهاجم على علم بالعمليّات الدّاخلية للجهاز؛ يستطيع إرسال إشارةٍ قويّة في اللحظة نفسها لحدوث عمليّة أمنيّة مُهِمّة. مثال ذلك عند التحقّق من هُويّة وكلمة السّر في جهاز ما، يُرسِل المهاجم إشارته القويّة في لحظة التحقّق نفسها، فتؤثّر هذه الإشارة في بعض الأجهزة، وبذلك لا تنفَّذ العمليَة، وتنتقل إلى العمليّة التي تليها؛ بحيث تحقّق مَطْلبَ المهاجم بالدخول إلى واجهة الجهاز، شكل (٢)، وعند الوصول لتنفيذ العمليّة (٣) (وهي التحقّق من أنّ المدخل لا يساوي صفرًا) يستطيع المهاجم أن يُرسِل إشارته القويّة؛ بحيث تعطِّل فعاليّة الجهاز للحظة، وهي كافية لجعله يقفز ولا ينفّذ عمليّة(٣). وسيكمل البرنامج والمتغيّر(a) يحتوي قيمة صفر أو أيّ قيمة خاطئة، في حين هجومُ الطّاقة (Power Glitching) يختلف قليلًا؛ بحيث تُرْسل إشارة قويّة عند وقت قراءة متغيّر من الذّاكرة؛ بحيث يأخذ المتغيّر قيمة خاطئة؛ مؤدّيًا إلى احتماليّة تعطُّل عمل الجهاز.

- **الهجوم باستخدام درجات حرارة عالية أو مُنخفضة (Temperature Attacks):** إذ يُعَرَّض جهاز التّشفير لدرجات منخفضة جدًا؛ ليتجمّد المُعالِج لوقت؛ بحيث يستطيع المهاجم استخراج المفاتيح من الترانزسترات الدّاخلية أو خلايا الذّاكرة الدّائمة (Memory Cells). ويعتمد هذا الهجوم بصورة كبيرة على سرعة المهاجم في استخراج الذّاكرة قبل حذف البيانات من وحدة التشفير. وقد أظهرت دراساتٌ حديثة إمكانيّة استخراج المفاتيح من الذاكرة العشوائية، إذا بُرِّدَتْ، واستطاع المهاجم فتحَ الجهاز وتوصيل الذاكرة في حاسوب قبل حذف البيانات.

```
Typical data output routine in security software:
1  b = answer_address
2  a = answer_length
3  if (a == 0) goto 8
4  transmit(*b)
5  b = b + 1
6  a = a - 1
7  goto 3
8  ...
```

■ شكل (٢) مثال لهجوم التوقيت.

● **الهَجَمات الهجينة**

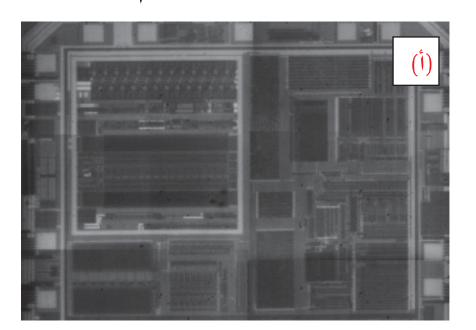
تُعَدّ الهجمات الهجينة (Semi-Invasive Attacks) مزيجًا بين الهجمات التخريبيّة وغير التخريبيّة، وقد ظهرت تقنيات حديثة تدعم وتساعد في تطوير مثل هذه الهجمات واكتشافها، وأصبحت تشكّل مجالًا خصبًا للبحث؛ لأنّها تمثّل حلًّا وسَطًا؛ من حيث: السّعر، والوقت، والأداء. ومن أشهر هذه الهجمات ما يلي:

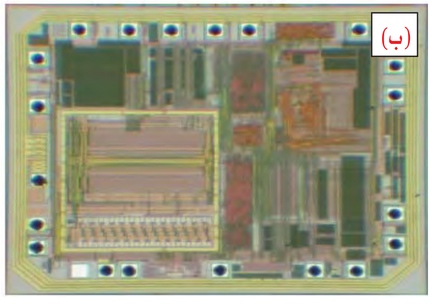
■ **هجوم الأشعّة فوق البنفسجية (UltraViolet Attacks):** وظهر في أواسط السبعينيّات الميلاديّة؛ بحيث يُسلَّط نور عالي الفولت (UV light) على الصّمام الكهربائيّ المسؤول عن أمْن الجهاز (Security Fuse) لتعطيله؛ ما يؤدّي لإعادة تشغيله في وضع غير آمن؛ لعدم فعاليّة الصّمام المسؤول عن حماية الجهاز.

■ **التصوير الخلفيّ للشّريحة (Backside Imaging):** وهو نسْخُ الجهة الخلفيّة للشّريحة - باستخدام أشعّة تحتوي فوتونات عالية الطاقة- لتعطيَ طريقةً أسهل لتحليل الشّريحة والمعالج، ومراقبتها من جهتها الخلفية؛ وذلك لأنّ مادة السيليكون تتميّز بشفافيّة عند تعرّضها لفوتونات صغيرة، ويوضّح الشكل (٣) صورة لشريحة مُصَوَّرة، وصورة التصوير الخلفيّ لها، ومدى دقّة الصورة؛ بحيث تمَكِّنُ المهاجِمَ من تحديد مكوّناتها الداخلية جميعها، الذي يُؤدّي إلى سهولة مُهاجَمَتها.

■ **هجوم اكتشاف الأخطاء (Fault Injection Attacks):** وهو تغييرٌ في حالة بعض الخلايا في الذاكرة، وتغيير القيم المخزَّنة فيها، سواء في الذّاكرة العشوائيّة أم غيرها من الذاكرات، وقد اكتسب هذا الهجوم انتشارًا كبيرًا؛ لقوّة تأثيره في أداء الجهاز، وتحكّم المُهاجم في تغييرات داخليّة في الوحدة.

■ **هجوم فحص الأيونات النّشطة (Active Photon Probing):** ويتعامل مع أيونات الدّوائر الداخليّة (Integrated Circuit-IC)، وكيفيّة تعاملها مع الشّعاع المُرْسَل، وتوجد عدّة تقنيات متقدّمة لتنفيذ هذا الهجوم.





■ شكل (٣) صورة لشريحة مُصوَّرة (أ)، وصورة للتصوير الخلفيّ لها (ب).

طرق الحماية من الهَجَمات

هناك عدّة طرق لتجنُّب مخاطر الهجمات أو تقليلها، من خلال التفكير العميق، واتّخاذ الإجراءات الأمنيّة اللازمة قبل تصميم جهاز التّشفير أو الأجهزة الحسّاسة، ويجب عمل الاختبارات اللازمة في أثناء تطوير الجهاز؛ للتحقّق من مدى فعاليّة هذه الطرق في صدّ الهجمات. ويمكن تقسيم هذه الدفاعات أربعة أقسام، هي:

● **دفاعات الواجهات الخارجيّة للجهاز**

تشتمل دفاعات الواجهات الخارجيّة للجهاز (External Interfaces Defense)، على:

- التأكد والتحقّق منْ كون المعلومات الحسّاسة المُرْسَلة للخارج دائماً مُشَفَّرة.

- التأكّد من إزالة واجهات الاختبارات (Test Interfaces) المُستخدَمة أثناء تطوير الجهاز وتصنيعه؛ لاحتوائها رسائل تفصيليّة عن الأخطاء، ولعدم مراعاة جانب الأمان فيها؛ بحيث يستطيع المُهاجم الاستفادةَ من هذه الواجهات لتحليل الجهاز.

- تجهيز الجهاز للتّعامل مع البيانات غير السّليمة الدّاخلة إلى الجهاز؛ بغرض التّخريب، ولاكتشاف مواضع الضّعف في الجهاز، مثل إرسال بيانات مغلوطة (Bad Packets).

- التقليل من أنواع الاتصالات المكنة في الجهاز قدر الإمكان، مثال عدم إضافة خاصيات نقل البيانات المعروفة كالبلوتوث والشبكات اللاسلكيّة الا للضرورة.

● **دفاعات الغطاء الخارجيّ**

تنقسم دفاعات الغطاء الخارجيّ (Enclosure)، إلى نوعين، هما:

■ **آليّات منع التلاعب (Tamper Mechanisms):** وتُستخدَم لمَنْع أيّ تدخّل فيزيائيّ مباشَر أو إلكتروني أو اكتشافه، أو محاولة العبث بالجهاز، وتُعَدّ هذه الآليّة من أهمّ الوسائل لحماية الجهاز من الهجمات الخارجية جميعها؛ وذلك لأنّ وصولَ المُهاجم للأجزاء الدّاخلية إلى الجهاز يُعَدّ خطورة كبيرة؛ بحيث يُسَهّل عليه اكتشاف المعلومات السريّة إذا استطاع الوصول المباشَر للذاكرة الداخليّة. وتنقسم هذه الآليّات إلى أربعة أقسام تكامليّة؛ بحيث تُستخدَم جميعها في حالة الأجهزة ذات الحساسيّة العالية، ويُعْتَمَدُ نوعُ المنع وآليَّته بحسب مدى أهمّية الجهاز والمعلومات المخزّنة في داخله وحساسيّتها، وتتمثّل هذه الآليّات في أربعة أنواع، هي:

- **مقاومة العبث (Tamper Resistance):** وذلك باستخدام موادَّ خاصّة؛ لزيادة الصّعوبة في فتح الغطاء والدخول إلى الجهاز، مع العلم أنّ هذه الطريقة لا تمنع من الدّخول إلى الجهاز، وعادة تُستخدَم للأجهزة غير الحسّاسة، ومنها: استخدامُ مسامير لا تستخدم كثيرًا، ووضع غطاء بلاستيكيّ مُقوًّى أو حديد، والتّصميغ الحراريّ للغطاء من المصنع، إلّا أنّ هذه الطرق جميعها لا تمنع من فتح الجهاز، لكنّها تزيد من صعوبة ذلك على الأقلّ.

- **دليل العَبث (Tamper Evidence):** ويتمثّل في وجود دليلٍ مرئيّ على أيّ محاولة عبث أو فتح للجهاز، وذلك عن طريق ختم الجهاز بشريط لاصقٍ حول الغطاء الخارجيّ، أو تصميغ الأجزاء مع بعضها بعضًا؛ بحيث إنه عند أيّ محاولة عبث فلا بدّ من كسر هذا الشريط أو الصمغ أو قطعه، وفي دراسة حديثة اُخْتُبِرَ ٩٤ نوعًا، وفُكّتْ جميعًا بوسائل وبأجهزة عادية.

- **اكتشاف العبث (Tamper Detection):** وهي خاصّية اكتشاف ومعرفة حدوث العبث مباشرة من الجهاز نفسه، وليس من المستخدم، أي أنّ جهاز التشفير يحتوي داخليًا حسّاسات دقيقة جدًا تساعده في اكتشاف أيّ محاولة عبث في مكنوناته الداخلة، أو محاولة فكّ الغطاء، ولكنْ لا يتصرّف الجهاز بأيّ ردة فعل، وتنقسم إلى :

١- اكتشاف محاولة العبث المباشَر إمّا عن طريق محاولة فتح الجهاز أو تحريك وحداته الداخلية. ويُستخدَم لاكتشاف هذه المحاولات حسّاساتٌ مغناطيسيّةٌ أو زئبقيّةٌ.

٢- اكتشاف محاولات التّأثير في الجهاز بعواملَ بيئيّةٍ خارجة عن المألوف: وذلك باستخدام حسّاسات تُسْتَخْدَمُ لقياس الحرارة أو الأشعّة أو الطّاقة أو التيّار الكهربائي؛ إذ يُوضَع معيارُ قياسٍ

للحسّاس، وأيّ ارتفاع على المستوى المطلوب يُنَبِّه عليه، أو عند حدوث تغيّر مفاجئ في إحدى هذه الظواهر يُكْتَشَف، وتكمن أهميّة هذه الحساسات؛ في منع هجمات الـ (Glitching) وهجمات الـ (X-Ray) وهجمات تبريد الذاكرة وغيرها.

٣- استخدام دوائرُ كهربائيّة (Circuitry) دقيقة جدًّا تحيط بالوحدات الحسّاسة؛ لاكتشاف أيّ محاولة عبث بحيث تستمرّ الإشارة الكهربائيّة في الدائرة، وعند حدوث أيّ تدخّل من أيّ جهة توَقف هذه الإشارة، ويَكتشف الجهاز هذه المحاولة، وتعدّ هذه أفضلَ الطّرق لاكتشاف محاولات الوصول المباشَر في الجهاز.

- **ردّة الفعل لمحاولات العبث (Tamper Response):** وتُعَدّ من أهمّ الوظائف لحماية الجهاز، وتحدث بعد اكتشاف محاولة عبث في الجهاز باستخدام أيّ وسيلة من الوسائل المذكورة أعلاه؛ فلا تستطيع ردّ محاولة العبث إلّا بوجود هذه الطرق. وتكمن أهميّتها في استطاعة الجهاز حمايةَ البيانات المُهمّة قبل أن يستخلصها المُهاجم، وهذا هو الهدف الأساسيّ المراد حمايته. وتتكوّن ردّود الفعل في الغالب من:

١- حلّ سلميّ؛ بحيث تُمْسَح البيانات الحسّاسة ومفاتيح التّشفير في ذاكرة الجهاز الدائمة والمؤقّتة؛ ممّا يجعل فتح الجهاز بدون أيّ قيمة، ولا يفيد المُهاجِم. مما يؤدّي إلى تعطّل وظائف الجهاز؛ لعدم وجود مفاتيح التّشفير.

٢- حلّ عنيف بتفجير محتوَى الجهاز بالكامل.

علمًا أنّ الحلّ الأوّلَ هو الغالب في الأجهزة مع وجود بعض الأمثلة على الحلّ الثاني في حالة استخدام هذه الأجهزة في الحروب، لكنْ يَجِبُ أن تكون هذه الاكتشافات مختبرة ومجرَّبة بعناية؛ لكي لا تمسَح البيانات أو ينفجر الجهاز بالخطأ.

■ **الوقاية من الإشعاعات:** إذ تبثّ الأجهزة الإلكترونية جميعها -دون استثناء- أشعّة كهرومغناطيسيّة (Electromagnetic Interface-EMI)، بطريقة عفويّة وغير مقصودة، لكنّها موجودة في خصائص الأجهزة، ولا نستطيع أن نمنع إرسالها؛ فيستطيع مُهاجِم المراقبة لهذه الإشعاعات، واكتشاف معلومات حسّاسة واكتشافها من مفاتيح التشفير، أو معرفة بيانات من شاشة الجهاز، وتنطبق أيضًا على أشعّة تردّدات الراديو (Radio Frequency).

وتتمثّل الدّفاعات المُسْتَخْدَمَة في وضع درع واقٍ (EMI Shielding)؛ وذلك لتحقيق ما يلي:

- المنع من انبثاق هذه الأشعة؛ مما يقلّل من الأشعّة المنبعثة من الجهاز، وتزيد من حصانته؛ إذ يمنع هذا الإجراء من هجمات تحليلِ الإشارات الكهرومغناطيسية.

- المنع من دخول أشعة كهرومغناطيسيّة عالية القوّة؛ مما يؤثّر في الجهاز وفي أداء وظائفه.

● **دفاعات وحدات المُعالَجة**

تشتمل دفاعات وحدات المعالجة (Circuit Board) على الآتي:

- إزالة أيّ مُلْصَق أو رقم تسلسليّ من على أجزاء اللّوحة نفسها، الذي يدلّ على نوع المكوّنات الموجودة على اللوحة مثل الـ(IC) أو الذاكرة التي فور معرفتها يَستطيع المُهاجم معرفةَ خصائصها، وعمل التّحليل المناسب لاكتشاف الثّغرات الأمنيّة.

- إزالة أيّ نقاط اختبارات وُضعت وقتَ تطوير الجهاز؛ لكي لا يستغلّها المهاجمون؛ لأنها تُعَدّ ثغرة، ولها وصول مباشَرٌ للذاكرة، وأجزاء أخرى حسّاسة للجهاز.

- حماية ناقل البيانات (BUS) وخطوط التحكم الدّاخليّة؛ لأنّها تمثّل أسهلَ أجزاءِ الوَحدة في الفحص والتّحليل.

- التّعامل بحذر مع ذاكرة وحدة المعالجة الداخليّة القابلة للتّعديل (Field-Programmable Gate Array-FPGA) لما تحتويها من تحميل الإعدادات عن طريق مصادر خارجيّة؛ بحيث يجب التّحقق من المصدر عن طريق شهادة المصادقة (Digital certificates) والتأكّد من عدم تغيير الملفّ المُدْخَل (Integrity).

- الوقاية من هجمات الإدخال والإخراج، وهي الهجمات التي يَستخدِم فيها المُهاجِم التركيباتُ المكنةُ جميعها للبيانات الدّاخلة إلى لجهاز، ومشاهدة نتائجها وتحليلها؛ لاكتشاف أيّ جزء يُعَدّ من مناطق الضعف في الوحدة.

- وضع حدود عُليا ودنيا للظروف التشغيليّة للجهاز من ناحية الطاقة الداخلة والخارجة، والتقليل من الفروقات في الطّاقة المتنقّلة داخل الوحدات؛ لمنع هجمات تحليل الطّاقة (Power Analysis).

- تقسيم الأجزاء وتوزيعها؛ من حيث قوّة الإشعاعات المنبعثة؛ بحيث تساعد في تقليل نسبة انبعاث الأشعّة من الجهاز.

- مراقبة إشارات تزامن الوقت والتحكّم بها (Clock Signals) ومحاولة الموازنة بين الوقت اللازم لكلّ عمليّة؛ وذلك لتجنّب هجمات الوقت (Timing Attacks).

- نقل معالج التشفير من البرنامج الداخلي المتحكِّم في باقي مكوّنات الجهاز (Firmware) إلى (FPGA)؛ لصعوبة فحصه مجهريًّا، ولزيادة أداء المعالج بصورة عامّة، أو استخدام وحدة معالجة خاصّة للتّشفير (Cryptographic Processor)؛ بحيث يكون فيها سبل الحماية والأمان المدرجة جميعها، ومنها: ردّة الفعل للعبث (Tamper Response)، ووحدة التحقّق من الهُويّة، وتوليد أرقام عشوائيّة داخليّة. ويَسْهُل التّعامل مع وحدات من هذا النوع؛ لوجود أوامر اتّصال واضحة وجاهزة للعمل، وأيضًا لاستخدامها إجراءات أمنيّةً جرّبها الخبراء واختبروها.

- اختيار خوارزميّات تشفير مُناسبة، وتعترف بها منظّماتٌ مُعتَرَفٌ بها كمنظّمة (National Institute of Standards & Technology-NIST)، وتطبيقها بطريقة تضمَن أداء الخوارزمية بالصورة المطلوب منها.

● **دفاعات الفيرموير**

تنقسم دفاعات البرنامج الداخلي المتحكّم في باقي مكوّنات الجهاز (Firmware) إلى ثلاثة أقسام، هي:

■ **كيفيّة تخزين المفاتيح**: وتتمثّل في:

- تشفير المفاتيح السريّة والحسّاسة في الذاكرة الدائمة أيًّا كان نوعها، وعدم فكّ تشفيرها إلّا بعد نقلها إلى الذّاكرة المؤقّتة، وعند الحاجة فقط، ومسحها بعد الانتهاء منها.

- عدم استخدام عنوان الذاكرة نفسه للمفتاح؛ لكي لا يتمكَّنَ مُهاجِمٌ ما من تحليل الخوارزميّة، ومعرفة موقع المفتاح واكتشافه، وإضافة إلى ذلك لا يتكوّن باقٍ من البيانات مطبوع مغناطيسيًّا؛ إذ أظهرت الدّراسات إمكانيّة اكتشاف مثل هذه الحالات؛ ولذلك يُنْصَح باستخدام تقنية التقليب (Flip-Flop) لكلّ ٣-٥ ثوانٍ.

■ **تحميل الفيرموير**، ويتمّ من خلال:

- أن لا يحُمَل أيّ فيرموير على الجهاز إلّا أن يكون مُوَقَّعًا إلكترونيًّا من مصدر موثوق ومعروف إذ يجب التحقّق من مصدره أوّلًا، وذلك باستخدام إحدى خوارزميّات التّوقيع الإلكتروني المعتَمَدة (Digital Signature Algorithm-DSA)، ومن ثمّ باستخدام خوارزميّات تشفير ذي الاتجاه الواحد (Hash) المعتمَدَة، مثل (SHA-2)؛ وذلك لتجنّب تنزيل أيّ فيرموير مُعَدَّل عليه.

- أن لا يتمّ نقل الفيرموير إلّا مُشَفّرًا؛ لكي لا يستطيع مُهاجِمٌ اعتراضَه، وتحليله، واكتشاف الثّغرات فيه.

■ **أساليب البرمجة الآمنة**، وتشتمل على:

- استخدام إعادة تمثيل (Encode) للبيانات ذات القيم الثابتة، وذلك في برمجية الفيرموير.

- إضافة متغيّرات وهميّة، وإضافة عمليّات، وبعض العمليّات الشَّرْطيـّة؛ لكي يُضَعِّف من فرص مهاجم في فهم البرنامج وتحليله.

- التحقّق والتأكّد من عدم وجود عيوب أَمْنيّة أو ثغرات واضحة في برمجة الفيرموير.

معايير أمنيّة دُوَليّة لتقييم أجهزة التشفير

بعد التطرّق إلى أنواع الدّفاعات يتبيّن أنّ مُعظمَها تحتاج إلى مهارة تقنية عالية، وأجهزة خاصّة عالية التكاليف؛ لتحليل الهجمات ومواكبة كلّ جديد في علم أمن المعلومات. وتُعَدّ أغلب هذه المواصفات بعيدة المنال، أو يصعب الحصول عليها في أغلب الشركات والقطاعات؛ فلذلك وُجِدَتْ معاييرُ ومَعاملُ دوليّة؛ لأجراء مثل هذه الاختبارات، والتحقّق من أساليب الحماية، وقياس قوّتها وفعاليّتها. وتُدير هذه المعايير مُنشَأة ذات سمعة، ومعروفة على المستوى الدّولي، ومن هذه المعايير: معيار معالجة المعلومات الاتحادية (Federal Information Processing Standard-FIPs)، ومعايير عامة (Common criteria-CC).

تُقيّم المعاييرُ أداء جهاز التّشفير و وظائفه، بناءً على خصائصه الأمنيّة، ومدى قوّة دفاعاته وصلابته أمام أنواع الهجمات المذكورة جميعها في هذا المقال. لنأخذ (FIPS) مثالًا، يوجد حاليًّا (١١) مجالًا أو منطقةً يركّز عليها معيار (FIPS 140-3) المعدَّل، وأهمّ هذه المجالات هي:

١- التأكّد من أنّ جميع الخوارزميات وجميع تقنيات التشفير التّابعة لها من إنشاء التّوقيع الإلكتروني وغيرها مُتوافِقَة مع مِقْياس (NIST).

٢- التأكّد من وجود آليّة للتحقّق من عدم العبث بالفيرموير، سواء أكان بالتّوقيع الالكتروني أم باستخدام الهاش (HASH).

٣- قياس قوّة دفاعات الأجهزة أمام الهجمات غير التخريبيّة (Non-Invasive Attacks).

٤- كيفيّة إدارة المفاتيح السريّة والمعلومات الحسّاسة ونقلها وتخزينها أثناء المدّة التشغيليّة للجهاز.

٥- ما أساليب الحماية من الهجمات الفيزيائيّة المباشرة (Physical Attacks)؟ وهل تحتوي تقنية تمنع من العبث (Tamper)؟.

يُعطي الجهاز تقييمًا من ١-٤ لكلّ منطقة من المناطق الـ(١١) بناءً على معايير ثابتة ومفصَّلة، وتُقَيّم المستويات جميعًا من هذه المناطق، ويُعطَى الجهازُ المستوَى المناسِبَ له، مع تقرير مُفصَّل بنتائجِ هذه الاختبارات.

الخـــاتمـــة

تُقاس قوّة أمن الشبكات والمعلومات بناء على قوّة أجهزة التشفير وأنظمة الأمان نفسها وصلابتها، وكيفيّة تطبيقها؛ إذ تَعْتَمِدُ المعاييرُ الحاليّة لقياس قوّتها -في الغالب- على قوّة خوارزميّات التشفير وحجم المفاتيح المستخدمة فيها فقط، ويُهْمَل جانبٌ كبيرٌ في التقييم ألَا وهو الهجمات الحديثة والمتطوّرة، وكيفيّة الدفاع عنها ؛ فبناء على دراسات الخبراء في مجال أمن المعلومات ستكون هذه الهجمات هي المُوَجِّه الأساس الذي يستخدمه المخرِّبون والهاكرز، التي يجب أن تُؤخذ بعين الاعتبار في التّقييم، وأيضًا عمل اللّازم في البَدْء لمبادرة لتخصيص الشّباب المُهْتَمّ في أمن المعلومات في هذه المجالات وتأهيلهم.

المراجع

- Physical Security Devices for computer Subsystems: A survay of Attacks and Defenses.2008 Weingart.F

-Power analysis attack Countermeasures and their weaknesses.2000. T.S Messerge

-Practical Secure Hardware Design for Embedded Systems..2004 Grand. J

- Semi-invasive attacks. A new approach to hardware security analysis.2005.Skorobogatov.S

-Semi-invasive extension to physical attacks.,2006 Skorobogatov .S

المحتوى الإلكتروني لطبقة الأيونوسفير في المملكة العربية السعودية

د. عبد العزيز بن عثمان العثمان



أدّى التطوّر الهائل في تقنيات الفضاء إلى زيادة استخدام الفضاء الخارجيّ بوصفه وَسَطًا ناقلًا للمعلومات من الأرض وإليها؛ إذ تنقل الأقمارُ الاصطناعيّة (GPS) هذه المعلومات بصورة متزايدة؛ لاستخدامها في أغراض مُتعدّدة، منها: الاتّصالات، والملاحة، والجيوديسيا (Geodesy) والطّقس، والاستطلاع، وغيرها من التّطبيقات الأخرى. كما انتشر في مجال الملاحة استعمالُ إشارات النّظام العالميّ لتحديد المَواقع (Global Navigation Satellite System-GNSS/GPS) على نطاق واسع على مستوى الأفراد والهيئات، وأصبح أداةً ضروريّةً لا يُستَغنى عنها، سواءٌ في الملاحة وتحديد المواقع أم في تطبيقات علميّة أخرى، مثل: دراسة الفضاء، وطبقة الأيونوسفير، وتحرّكات القشرة الأرضيّة، والجيوديسيا، وغيرها.

تعتَمِدُ فِكْرَةُ القياس بنظام الأقمار الاصطناعيّة -يتكوّن من ثلاث وحدات رئيسة: هي وحدة الفضاء ووحدة التحكّم، ووحدة الاستقبال- أساسًا على قياس الموجات (Signals) التي تَبُثُّها تلك الأقمارُ ورصدها، من ارتفاع يصل إلى قرابة ٢٠,٠٠٠ كم إلى المُستخدِمين كافّة في العالم، في أيّ زمان ومكان، وتمرّ هذه الموجات خلالَ طبقات الغلاف الجويّ (Atmosphere) التي بدَوْرها تؤثّر فيها؛ مما قد يؤدّي إلى تعطيلها، وربّما تأخير وصولها إلى المُستخدِمين، وبذلك تقليل دقّة الرّصد والملاحة.

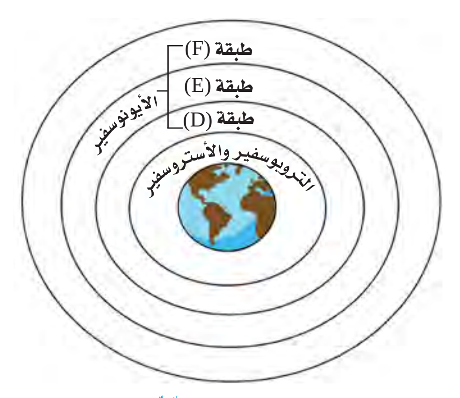
من ناحية أخرى فإنّ طبقات الغلاف الجويّ تُحْدِث أحيانًا تأثيرًا سلبيًا في الاتّصالات اللاسلكيّة، وخصوصًا الإشارات ذات التردّد العالي (HF,VHF) القادرة على نقل معلوماتٍ كثيرة. ونظرًا إلى الموقع الجغرافيّ للمملكة، ووقوعها في منطقة تغيّرات حراريّة استوائيّة؛ فإنّه يُتَوَقَّع أن يَحْدُثَ في تلك المنطقة ما يُسَمَّى الشّذّات الاستوائيّة المتأيّنة (Equatorial Ionized Anomaly- EIA) التي من خصائصها انخفاضُ كثافة الأيونات عند اقترابها من خطّ الاستواء؛ إذ تكون هناك قيم الـ (EIA) مُرتفِعة ومُتماثِلة حول خطّ الاستواء.

تُعَدّ دراسة الغلاف الجَوّيّ مفيدةً لجهات عديدة في المملكة، منها: الطّيران المَدَنيّ، والمؤسّسة العامّة للموانئ، ووزارة الداخليّة، ووزارة الدفاع، وجهات أخرى؛ نظرًا لتأثيرها في الملاحة، وتحديد المواقع، والاتّصالات.

يقدّم هذا المقال تعريفًا لطبقة الأيونوسفير (Ionosphere) ومدى تأثيرها في الملاحة وتحديد المواقع. كما سَتُوَضَّحُ نتائجُ دراسةٍ تمّت؛ لمعرفة التغيّرات التي حدثت في طبقة الأيونوسفير في المملكة في مدّة زمنيّة مُحدَّدة، باستخدام أجهزة استقبال (Receivers) لإشارات الأقمار الاصطناعيّة للملاحة وتحديد المواقع (GPS).

طبقة الأيونوسفير

تُمثّل طبقة الأيونوسفير (Ionosphere) الطّبقةَ العُليا من الغلاف الجوّيّ (Atmosphere)، وتمتدّ من ارتفاع ٥٠ كم فوق سطح الأرض إلى أكثر من ١٠٠٠ كم، ويَحْدُثُ فيها عمليّاتُ تأيّنٍ للذرّات؛ ما يؤدّي إلى تشتّت مسار موجات الراديو وإشاراته التي تمرّ من خلالها؛ وذلك لأنّ مُعامل انكسار تلك الموجات دالّةٌ رياضيّة تتأثّر بكلٍّ مِنْ: تردّد الإلكترونات ومجموعها (Total Electron Content-TEC) في وحدة مِتريّة (م٢) بطبقة الأيونوسفير. يتغيّر مجموع الإلكترونات (TEC) تغيّرات قويّةً ومتفاوتة مع الزمن بمعدّلٍ يوميّ، وشهريّ، وموسميّ، وسنويّ.

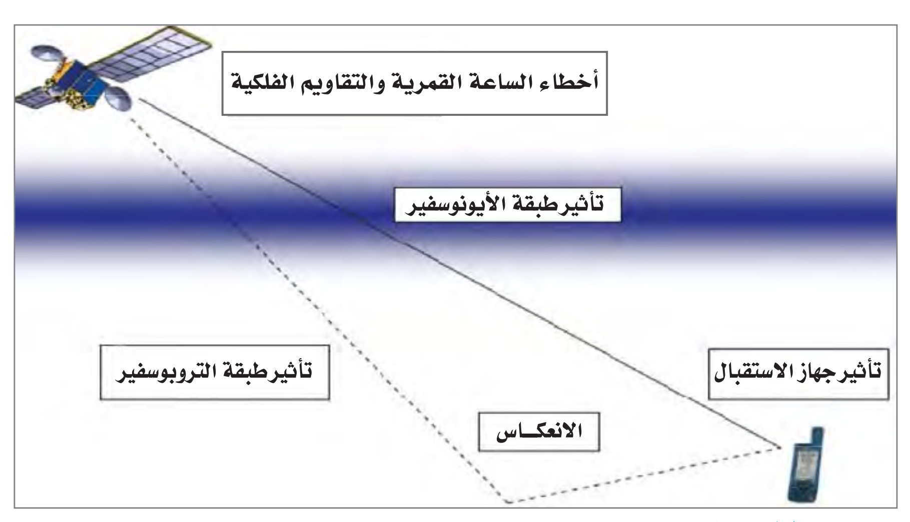


■ شكل (١) طبقات الغلاف الجوّيّ (Atmosphere) .

تنقسم طبقة الأيونوسفير - حسب كثافة الإلكترونات فيها - إلى ثلاث طبقات، شكل (١) هي:

- طبقة (D): ويبلغ سمكها أكثر من ٥٠ كم، وتمثّل أقلَّ الطَبقات كثافةً.
- طبقة (E): ويصل سمكها إلى أكثر من ٩٠ كم، وهي متوسّطة الكثافة.
- طبقة (F): وهي أعلى الطّبقات، ويصل سمكها إلى أكثر من ١٥٠ كم، كما أنّها أعلى الطّبقات كثافةً.

يُعَدّ المُحتوَى الإلكتروني (TEC) الوحدةَ الأهمّ لوصف كثافة الإلكترونات في مسار حزمة الأشعّة والموجات المراد قياسها، وتمثّل الوحدة الواحدة (TECU) بعدد يساوي ١٠^١٦ إلكترون محسوبةً في أسطوانة مساحة مَقْطَعِها ١م٢ ممتدّة على طول مسار الأشعّة. تُعَدّ الأشعة فوق البنفسجيّة (Ultraviolet) - جزءًا من أشعّة الشمس - المَصْدرَ الرّئيسَ لعمليّة تأين الذّرّات خلال ساعات اليوم والنهار؛ إذ يحدث انطلاق للإلكترونات من الذرّات؛ مما يؤدّي إلى انبعاث طاقة إشعاع ذريّة (Solar Radiation)، ويتأثّر مرور إشارات موجات الـ (GPS) بعدد (أو كثافة) الإلكترونات الحرّة المُنْبَعِثة من تلك الذرات، كما تعتمد كثافة الإلكترونات في طبقة الأيونوسفير من الغلاف الجوي



■ شكل (٢) مَصادر الأخطاء في نظام الملاحة (GPS).

على الوقت، والموقع الجغرافي والفصل من السنة، والنشاط المُصاحِب للدّورة الشّمسية (Solar Cycle).

● **تأثير الأيونوسفير**

تنعكسُ موجات الراديو ذات التردد الأقلّ من ٣٠ ميجا هيرتز من طبقة الأيونوسفير، كما تنعكسُ إشارات الملاحة بالأقمار الاصطناعيّة (GPS) التي تمر من خلالها، لذا تُعَدّ هذه الطبقة عاملًا مُشتَركًا للملاحة وتحديد المواقع بالأقمار الاصطناعيّة والاتصالات اللاسلكية. تتأثّر دقّة قياسات الأقمار الاصطناعيّة بعدّة مصادر، شكل (٢)، مُسَبِّبةً حدوث عدّة أخطاء في القياس، من أهمّها: تأثير الغلاف الجوّيّ (Ionosphere, Troposphere)، وساعة قياس الأقمار (Clock)، ونوع الجهاز المستخدم في القياس (Receiver)، ويوضّح الجدول (١) قِيَمًا تقريبيّة للتأثير المتوقَّع لبعض مصادر هذه الأخطاء؛ إذ يمثّل تأثير طبقة الأيونوسفير أكبرَ مصدرٍ للخطأ في القياس بالـ (GPS)، ويصل مقداره إلى عدّة أمتار، ومن المُمْكن استخدامُ أجهزة الاستقبال الأرضيّة المزدَوجة التردّد (Dual Frequency)؛ لرصد إشارات الأقمار الاصطناعيّة (GPS) التي تصل عبر الغلاف الجوي؛ للحصول على قيم (TEC) وبحث تغيّراتها الزّمنية والجغرافية، علمًا أنّ هذه الأجهزة بإمكانها قياسَ الكَمّ الأكبر من تأثير طبقة الأيونوسفير ذات الطبيعة التشتية للموجات واسترجاعَها.

ومن ناحية أخرى فإنّه عند استخدام موجات الـ (GPS) الأحاديّة التردّد (Single Frequency) في التطبيقات المساحيّة والجيوديسيّة الدّقيقة لحسابات شبكة قياس أرضيّة (Network) ذات عدد من نقاط الاستقبال، فإن ذلك سيؤدّي إلى تشوّه في الشبكة المحسوبة؛ نتيجةً لتجاهل تأثير طبقة الأيونوسفير في تلك الموجات، وسيكون مقدار الخطأ (أي التقلّص) في خطّ الرّصْد (Baseline) بين كلّ نقطتين من نقاط الرّصد

مصدر الخطأ	الصيغة الكيميائية		الساعة	الجهاز	التقاويم الفلكية	الانعكاس
	تروبوسفير	أيونوسفير				
قيمة الخطأ (متر)	٠,٧	٤	٢,١	٠,٥	٢,١	١,٠

■ جدول (١) قيم تقريبيّة لبعض مصادر الأخطاء التي تؤثّر على دقة القياس بموجات الـ (GPS) .

حواليَّ ١ جزء في المليون (1ppm) أو ما يعادل مقدار ١سم في كل ١كم؛ مما يؤثّر سلبًا في أعمال المساحة ذات الدقة العالية. كما أفادت الدراسات أنّ القيَم العليا لتأثير الأيونوسفير في موجات الـ (GPS) تقع على ارتفاع يتراوح بين ٢٠٠– ٤٥٠ كم تقريبًا، في الطبقة (F) من الأيونوسفير.

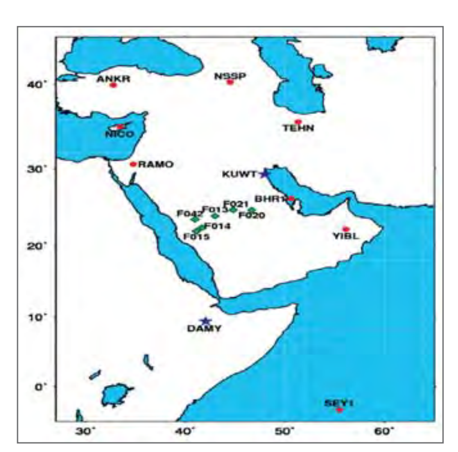
● **تأثير الأيونوسفير على الاتّصالات اللاسلكيّة**

ترسَل إشارات الاتصالات اللاسلكيّة – من موقع لآخر – من سطح الأرض إلى أعلى مباشَرةً؛ لتنعكسَ من طبقة الأيونوسفير في الغلاف الجوّيّ، شكل (٣) وتصل إلى الموقع المطلوب، ولا تُرْسَلُ هذه الإشارات إلى سطح الأرض؛ وذلك لتفادي مشكلة انحناء سطحها واختلاف طوبغرافيتها، الذي قد يؤثّر في حركة الإشارات، ويمنعها من الوصول إلى مكانها الصحيح. من ناحية أخرى تتأثّر إشاراتُ الاتّصالات اللاسلكيّة وموجاتُها بحالة الجوّ في الطّبقات المتوسِّطة (E) أو العُلْيا (F) من طبقات الأيونوسفير؛ ما يؤدّي إلى تشتّتها أو بعثرتها، وقد أدّى ذلك إلى تطوّر الاتّصالات بالأقمار الاصطناعيّة، ومع ذلك لم يُسْتَغْنَ عن الاتّصالات اللاسلكيّة، بل الاعتماد عليها مازال قائمًا في بعض الأحوال التي قد لا تتوافر فيها الأقمار الاصطناعيّة.

حساب المحتوى الإلكتروني لطبقة الأيونوسفير بالمَملكة

تقع المملكة العَربيّة السّعوديّة في منطقة حراريّة شَمال منْطقة خطّ الاستواء، وتتميّز بتغيّرات حراريّة عاليّة؛ نتيجة لزيادة مدّة تعرّضها لحرارة الشّمس، ونظرًا إلى كبَر مساحة المملكة، وموقعها الجغرافي، وطول حدودها الساحليّة؛ فهناك حاجَة إلى حساب طبقة الأيونوسفير على مستوىً إقليميٍّ بدقّة أعلى من الحسابات الأخرى (العالميّة) ذات الطّابع العامّ (دقة أقلّ)؛ ليمثّل ذلك أساسًا لعمليّات الملاحة وتحديد المواقع والاتّصالات اللاسلكيّة، وغير ذلك من التطبيقات.

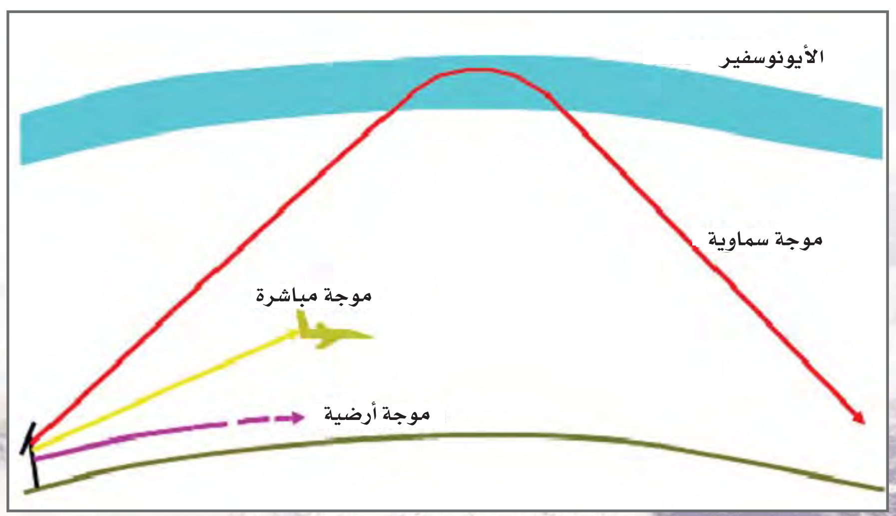
لمعرفة التغيّرات الزمنيّة التي تَحْدُثُ في قيم (TEC)، وبحث التّأثيرات الجغرافيّة عليها، فقد اُسْتُخْدِمَتْ أجهزة الاستقبال الأرضيّة مزدوجة التّردّد (Dual Frequency)؛ لرصد إشارات الأقمار الاصطناعيّة. وقد أُجْريت القياسات وجُمِعَت المعلومات ميدانيًا بمعدّل يوميّ للمدّة من ١–١١ فبراير ٢٠٠٩م، من خلال شبكة أرضيّة إقليميّة تتكوّن من ١٦ محطّةً من محطّات الاستقبال من الأقمار الاصطناعيّة، موزَّعة في منطقة الدّراسة وحولها، شكل (٤) وهي:



■ شكل (٤) توزيع نقاط الاستقبال المُسْتَخْدَمة في الدّراسة.

- ستة نقاط استقبال أرضيّة إقليميّة من نقاط الشبكة الجيوديسية الوطنيّة للمملكة حُصِلَ عليها من إدارة المساحة العسكريّة و وُضِعَت عليها أجهزةُ استقبال (GPS) من نوع (Trimble)؛ لاستخدامها في تسجيل الموجات باستمرار ولمدّة تسعة أيّام مُتواصلة.
- عشرة نقاط من النّقاط العالميّة (IGS) المُحيطة بمنطقة الدراسة للرّصد المستمرّ.

حُسِبَتْ قيم (TEC) في أوقات زمنيّة متتالية بمعدّل ساعتين لطبقة الأيونوسفير باستخدام القياس الصفريّ (Zero Difference)، والمُضاعَف (Double Difference) للموجات الحاملة لإشارات الأقمار الاصطناعية في منطقة الدراسة، وذلك باستخدام برنامج **برنيز** (BERNESE 5.0) المطوَّر في جامعة بيرن بسويسرا، مع تطبيق طريقة التّحديد الدقيق للمواقع (Precise Point Positioning-PPP)؛ لمعالجة تلك البيانات المُسجّلة لنقاط الـ (GPS) الإقليميّة والعالميّة في منطقة الدراسة وتحليلها. تتميّز تلك الطريقة بإمكانيّة معالجة قياسات وإشارات الأقمار الاصطناعيّة المَرْصُودة لكلّ موقع على حدة بدون الحاجة إلى الرّبط مع المواقع الأخرى. كما اُسْتُخْدِمَتْ مُنْتَجات المُنظَّمة الدُّوَليّة لخدمات أنظمة الملاحة العالميّة (International GNSS Service- IGS)،

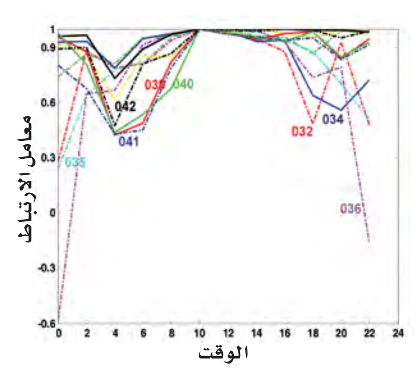


■ شكل (٣) نظام الاتّصالات اللاسلكيّة.

وطريقة (Geometry-free zero difference) للحصول على قيم (TEC) وتقدير الخطأ (RMS) بمعدَّل ساعتين على صورة شبكة (خارطة) بمسافة ٠,٥ x ٠,٥ درجة جغرافيّة. كذلك أُستُخدِمَتْ طريقة الطبقة الأحاديّة (Single Layer) لحساب المحتوى الإلكترونيّ (TEC) على ارتفاع ٣٥٠كم عن مستوى سطح الأرض، وتُعَدّ هذه الطريقة مناسبةً حينما تَكُوْن المسافات بين النقاط المعالّجة في الشبكة الإقليميّة ما بين (٥٠٠كم – ٢٠٠٠كم).

يُوَضّح الشكل (٥) القيم المَحْسُوبة للمحتوَى الإلكترونيّ في أوقات زمنيّة مقدارها ساعتان، ابتداءً من منتصف الليل ولمدّة ٢٤ ساعة في أحد الأيام، ويتّضح من الشّكل تناقصُ قيم المحتوَى الإلكتروني تدريجيًّا من ٥ إلى ١ وحدة قياس بين السّاعة ١٨:٠٠ إلى السّاعة ٠٢:٠٠ على التوالي، ثم تزداد تدريجيًّا حتّى السّاعة ٠٤:٠٠. ثمّ تتغيّر بسرعة لتصل ذروتها (١٧ وحدة) بين الساعة ٠٨:٠٠ والساعة ١٠:٠٠، وبعد ذلك تَنْخفض لتصلَ قيمتُها الصُّغرى إلى وحدة واحدة فقط في السّاعة ١٨:٠٠.

توضّح خرائط الشكل (٥) مدى اختلاف المحتوَى الإلكترونيّ حسب الوقت من اليوم، وكذلك اختلافه من موقع لآخر، كما تبيّن هذه الخرائط أنّ المملكة العربيّة السّعوديّة تقع في منطقة ذات تغيّر عالٍ في المحتوَى الإلكتروني، ولفهم التّغيرات اليوميّة فقد حُسِبَ مُعامل الارتباط (Correlation Factor) للقيم اليوميّة المَحْسوبة لتلك الخرائط لكلّ يوم من أيّام الدراسة موازنة مع قيمتها في السّاعة ١٠:٠٠ من كلّ يوم، شكل (٦).



■ شكل (٦) معامل الارتباط لقيم المحتوى الإلكتروني موازنة مع القيم في الساعة ١٠ من كل يوم .

الخلاصة

توضّح تلك الدراسة قيمة الشّذّات المتأيّنة الاستوائيّة جنوب خطّ عرض ٢٠ شمالاً؛ إذ يتّضح جليًّا ظُهورُ هذه الشّذّات في منتصف اليوم من السّاعة ٠٨:٠٠ إلى الساعة ١٦:٠٠ في جَنوب الجزيرة العربيّة. كما أظهرت تلك الدّراسة أنّ التغيّرات اليوميّة التي تحدث في قيم المحتوى الإلكتروني أكثر استقرارًا في النّهار موازنة مع المساء. وقد تمثّل هذه الدّراسة نواةً للنّظام التفاضليّ الإقليميّ للملاحة (DGPS) و(SBAS) للأغراض الجيوديسيّة والملاحة والاتّصالات في المملكة.

المراجع

- Alothman, A.O., Alsubaie, M.A., Ayhan, M.E., Short term variations of total electron content (TEC) fitting to a regional GPS network over the Kingdom of Saudi Arabia (KSA). Advances in Space Research 48 (2011) 842-849.

-Dach, R., Hugentobler, E., Fridez, P. , Meindl, M., (2007). Bernese GPS software Version 5.0. Astronomical Institute, University of Bern.

-Hansen, A.J. (2002). Tomographic estimation of the ionosphere using terrestrial GPS sensors. PhD Thesis, Dept. of Electric Eng., Stanford University, pp.200.

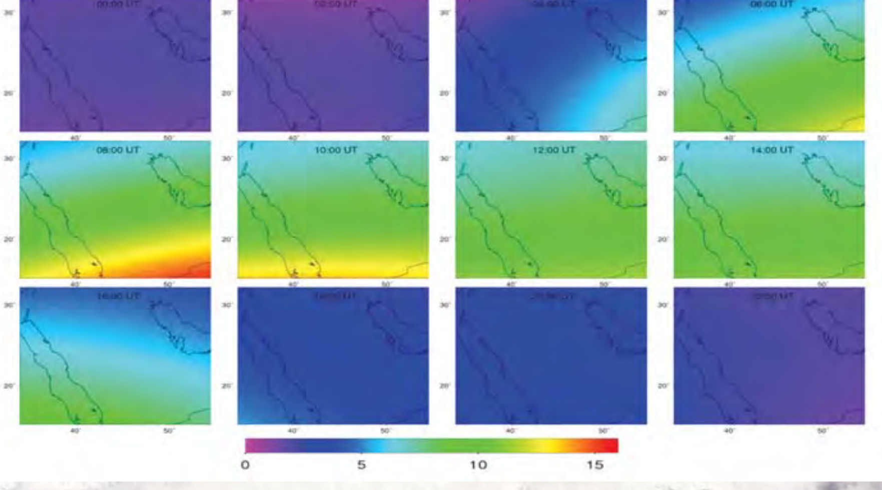
-Jakowski, N., Heise, S., Wehrenpfennning, S., TEC Monitoring by GPS – A possible contribution to space weather monitoring. Phys. Chim. Earth (C) 26, 609-613, 2001.

-Klobuchar, J.A. (1991). Ionospheric effects on GPS. GPS World, 2(4), 48-51.

-Schaer, S. (1999). Mapping and predicting the Earth's ionosphere using the Global Positioning System. Ph.D. Thesis, Astronomy Institute, University of Bern.

-Seeber, G. (2003). Satellite Geodesy: Foundations, Methods, and Applications, Walter de Gruyter, Berlin New York, ISBN: 3110175495, 589 pp.

-Wild, U. (1994), Ionosphere and Geodetic Satellite Systems: Permanent GPS Tracking Data for Modelling and Monitoring, Vol. 48 of Geodatisch-geophysikalische Arbeitenin der Schweiz, Ph.D thesis.



■ شكل (٥) خرائط المحتوى الإلكتروني المحسوبة لكل ساعتين في المملكة.

الإبداع في بيئة العمل البحثية

د. أماني الشاوي

تعد إدارة الموارد البشرية أحد أهم عوامل النجاح لأي مؤسسة سواء كانت ربحية أو غير ربحية؛ ولذلك فإنه من الضروري التركيز على تطوير قدرات ومهارات الموظفين لمواكبة التطور السريع في مجالات العلوم والتقنية، والتي لها الأثر الكبير في الحفاظ على الاستمرارية و جودة الأداء. ومن المعلوم أن استخدام وسائل جديدة ومميزة لتحفيز وتطوير الموارد البشرية يؤدي إلى تحقيق أعلى مستويات الإنتاجية والتميز. وقد أدركت الشركات والمؤسسات في جميع أنحاء العالم أهمية تشجيع الابتكار والإبداع في مكان العمل، كما لاحظت الشركات والمؤسسات التعليمية والمراكز البحثية المزايا العديدة لتحفيز عملية التفكير الإبداعي وتشجيع الموظفين لاقتراح أفكار جديدة ومبتكرة.

توفر نظم الابتكار المتكاملة حلولاً تقنية لإدارة الأفكار لمساعدة صناع القرار في تحويل الأفكار إلى منتجات أو خدمات أو عمليات تستفيد منها المؤسسة. ومع ذلك فإن عملية تشجيع الموظفين على التطوع بأفكارهم أصبحت تشكل تحديا لنظم الابتكار والشركات، وذلك لكثرة العوامل المؤثرة والمتأثرة بهذه العملية فضلاً عن صعوبة تنظيمها بشكل سلس يضمن الاستمرارية و الجودة في وقت واحد.

يعرض هذا المقال عددا من أنظمة إدارة الابتكار، مع التركيز على السياسات والإجراءات الإدارية الضرورية لتحقيق الأهداف المرجوة. بالإضافة إلى عدد من أدوات التقنية المثلة ببرمجيات مفتوحة المصدر يمكن أن تخدم أي نظام لإدارة الأفكار، وينتهي المقال بعرض لتجربة قسم الباحثات في مركز الإلكترونيات والاتصالات والضوئيات التابع **لمدينة الملك عبدالعزيز للعلوم والتقنية** في توظيف الخرائط الذهنية لتنظيم النشاطات المصاحبة للمؤتمرات العلمية التي تنظمها المدينة.

الإبداع والابتكار

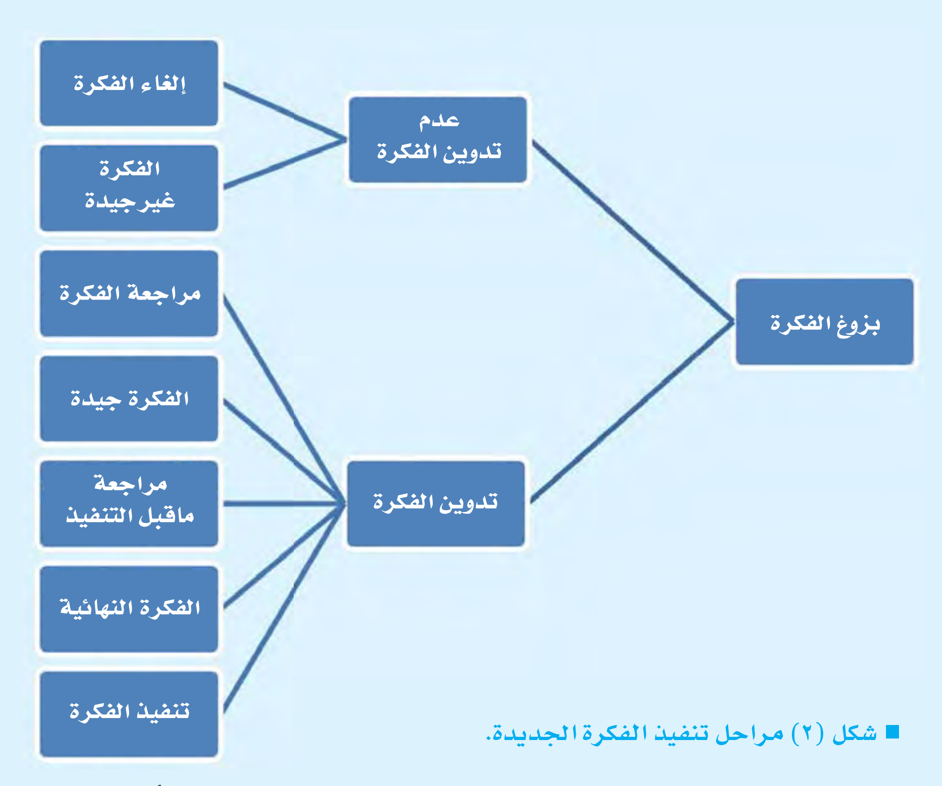
لمعرفة الفرق بين مفهوم الإبداع والابتكار فهناك العديد من التعاريف لكلٍ من هذين المفهومين، حيث تختلف النظرة لكلٍ منهما حسب المجال العلمي وظروف التطبيق. ولكن في بعض الأحيان قد تُستخدم كلتا الكلمتين للدلالة على نفس المفهوم.

يُعرّف الإبداع (Creativity) في اللغة بأنه اختراع الشيء على غير مثال سابق، والمبدع هو المنشئ أو المُحدث الذي لم يسبقه أحد. بينما الابتكار (Innovation) في اللغة هو المبادرة إلى الشيء، ويعرف بأنه عملية إنشاء الفكرة الجديدة أو التوصل إلى الفكرة الجديدة وتنفيذها وتوصيلها إلى السوق بعد أن يتم تحويلها إلى منتج ذي قيمة؛ أي يكون ذا منفعة ويشبع حاجة على مستوى الفرد أو الشركة.

يوضح الشكل (١) الإطار العام لدورة الابتكار المبنية على نموذج **إيقرز وسينق**



■ شكل (١) دورة الابتكار المبنية على نموذج إيقرز وسينق.



■ شكل (٢) مراحل تنفيذ الفكرة الجديدة.

التي تتميز بكونها عملية مستمرة تتعلم منها المنشأة من نشاطاتها الابداعية ومن تجارب الآخرين في مجالات العمل المشابهة.

ركّزت كثير من الأبحاث على توضيح أهم المراحل التي تمر بها الأفكار الجديدة من حيث التدوين والتقييم والمراجعة، و لعل من أشمل هذه النماذج المختصة بتطوير المشاريع الجديدة ما يوضحه الشكل (٢). حيث يشدد هذا النموذج على إعادة تقييم و مراجعة الأفكار في أكثر من مرحلة.

تشجيع الأفكار الجديدة في بيئة العمل

يُقَسّم المتخصصون - في مجال إدارة الأفكار - الحلول التي يمكن أن تُتَّبع لتشجيع الإبداع إلى قسمين هما:

● **حلول مؤسسية**

تتمثل الحلول المؤسسية في الآتي:

- تشجيع الإبداع في مجال مهم يخدم بشكل مباشر أهداف المنشأة الإستراتيجية.
- التحول - قدر الإمكان - من النظام الإداري المركزي إلى نظام تعاوني يرحب بأفكار الجميع.
- القيادة عن طريق طرح الأسئلة و تقييم البدائل المناسبة من غير فرض حلول جاهزة سهلة التطبيق.
- تحفيز فريق العمل و التأكيد على أهمية الأفكار المطروحة باستخدام أساليب بسيطة مثل الشكر و التقدير أو المحفزات المادية.
- استخدام الأسئلة المحفزة للتفكير الإبداعي مثل:

١- ماذا لو لم نستطع تطبيق...؟

٢- ماذا أيضا نستطيع أن نفعل بخصوص...؟

٣- لماذا لا نختار هذا الحل؟

و في مقال بعنوان «كيف نوفر بيئة عمل محفزة للإبداع» يرى مستشار الموارد البشرية **بندر الضبعان**، أن التنويع يعد من أهم العوامل المساعدة على تشجيع الإبداع في المنشآت و الشركات، و يذكر أن «تنوع القوى العاملة أحد أسباب نجاح المؤسسات؛ فإذا كان موظفو المؤسسة نسخاً مكررة من بعضهم البعض في الفكر والأسلوب الإداري والمؤهلات والخبرة، فمن المستبعد أن يخرج من بينهم من يفكر بطريقة إبداعية غير نمطية أو يرى الأمور من زوايا مغايرة»

● **حلول فردية**

قد يعمل الموظف أحياناً في منشأة لا تتبع سياسة محددة لتشجيع الإبداع، إلا أنه يستطيع أن يطبق أساليب بسيطة تساعده على تطوير مهاراته الإبداعية. مثال على ذلك: تطبيق مهارات إدارة الوقت والرياضة والعمل بشيء مختلف. وقد أثبتت دراسات كثيرة أن العمل في قسم جديد أو على مشروع يختلف تماما عما يقوم به الموظف طوال الوقت من شأنه أن يطور لديه التفكير الإبداعي بشكل كبير. ومن أهم الشركات التي تطبق هذا الأسلوب شركة جوجل التي تستخدم « قاعدة ٢٠٪» التي تنص على السماح للمهندسين بقضاء ٢٠٪ من أوقاتهم في العمل على أفكار ومشاريع مبنية على اهتماماتهم الشخصية، حيث كان لهذه القاعدة تأثير كبير على مخرجات الشركة مكّنتها من توليد - خلال هذا الوقت - تطبيقات عديدة من أهمها نظام البريد الإلكتروني (Gmail)، وكذلك أخبار جوجل (Google News).

خصائص نظام الابتكار

لا توجد صيغة عالمية بسيطة وناجحة لتحديد مسار عملية الابتكار وعناصرها الأكثر أهمية، فالابتكار في أي مؤسسة هو عملية مركبة تعمل على العديد من المستويات المتداخلة وتعتمد بشكل كامل على العنصر البشري، ويكاد يكون من المستحيل أن تعتمد بشكل تام على الحلول التقنية. ومع ذلك فإن الابتكار ليس عملية عشوائية، فهو مرتبط بشكل كبير بظروف المؤسسة في الماضي والحاضر وخططها المستقبلية.

تكمن أهم خصائص نظام الابتكار الناجح في جذب واستبقاء الموظفين المدربين ذوي المهارات العالية، وإتاحة الفرصة لهم للحصول على المعرفة، ومن ثم تشجيعهم وتمكينهم من التفكير والتصرف بشكل مبتكر. ويمكن تلخيص أهم خصائص نظام الابتكار الناجح بالنقاط الآتية:

- وضوح مهمة وأهداف المؤسسة، وتحديد عوامل النجاح والتزام الإدارة العليا بها.
- وجود بيئة عمل محفزة وداعمة للابتكار بجميع أشكاله تشجع على المخاطرة المحسوبة و تدعم موظفيها المبدعين و تشجعهم.
- نظام إداري منظم يستوعب أن الحاجة للابتكار هي جزء لا يتجزأ من عمل المؤسسة، و يستطيع تحليل المشاكل ومعرفة ارتباطها بكل جزء من أجزاء العمل و تفاعلها مع مشاريع المؤسسة.
- أن يكون الابتكار مسؤولية الجميع بدون استثناء خصوصا الإدارة العليا التي تضطلع بدور توفير الموارد المالية لدعم الابتكار.
- تأهيل موقع العمل بشكل يدعم أنشطة الابتكار بتوفير غرف اجتماعات مزودة بالتقنيات ووسائل الاتصال المناسبة لدعم اجتماعات ولقاءات فريق العمل و استقبال عملاء المؤسسة والتواصل معهم بشكل مباشر، كذلك من الضروري وجود غرف خاصة بالنشاطات الفردية التي قد تحتاج للهدوء والتفكير الإيجابي.
- توفير إجراءات الموارد البشرية التي تكفل للموظفين طرق التفكير والتعلم المتنوعة لدعم فكرة خلق حلول متعددة للمشكلة الواحدة من جميع وجهات النظر الممكنة.
- تكوين فرق العمل المتميزة بالتفكير الفردي وتجنب التفكير الجماعي والتي تحقق التوازن بين المبتدئين وذوي الخبرة، وتشجع على حرية الفكر مع الانضباط، والارتجال في التخطيط؛ ففرق العمل الناجحة هي التي تركز على أساليب التفكير المتنوعة و المهارات المختلفة للتعامل مع جميع التحديات التي تواجهها .
- الحفاظ على مستويات عالية من اللامركزية والتمايز الوظيفي ووجود مجموعة من المجالات المتخصصة الداعمة للعمل كمجموعة.
- الحرص على وجود نظام لإدارة المعرفة والعمليات التي تنتج باستمرار أفكارًا و مفاهيم جديدة.
- قياس أداء المؤسسة من ناحية دعم الإبداع والابتكار والتأكد من مراقبة وتقييم المدخلات والعمليات والمخرجات وأخذ هذا التقييم بعين الاعتبار عند تحديث النظام الإداري و تحديد الأهداف الاستراتيجية.



نظام إدارة الأفكار

نظام إدارة الأفكار (Idea Management System) هو نظام تتبعه المنشأة لجمع وتقييم أفكار ومقترحات الموظفين قد يكون نظاماً مبسطاً جداً يتمثل بوضع صندوق اقتراحات أو بريد إلكتروني في متناول الجميع، وقد يكون نظاماً إدارياً وتقنياً متكاملاً يسمح بطرح الأفكار ومناقشتها وتقييمها حسب معايير محددة متفق عليها مسبقاً. ومن الخدمات التي تقدمها أحدث أنظمة إدارة الأفكار العالمية ما يلي:

- وسائل تشجيع الإبداع وكيفية تطبيقها.
- طرق تجميع الأفكار من الموظفين.
- تقنيات العمل بروح الفريق.
- نظام التحفيز و المكافآت.
- أدوات تقييم و مراجعة الأفكار.
- آلية الحصول على التقارير الدورية والإحصاءات عن عمل النظام وفاعليته.

تبدأ عملية اختيار النظام المناسب لإدارة الأفكار بالتركيز على الهدف من تطبيقه: هل تسعى المنشأة لزيادة الأرباح؟ أو تقليل التكاليف؟ أم تهتم بالمحافظة على أداء مميز في بيئة تنافسية؟ بعد تحديد الهدف بدقة يجب البحث في الخدمات التي سيقدمها النظام للمستخدمين من حيث كيفية التعامل مع الأفكار والمقترحات وكذلك طريقة تقييمها. ومن ثم نستطيع أن نختار النظام المناسب مع الأخذ بعين الاعتبار المتطلبات التقنية لتطبيقه داخل المنشأة.

حلول تقنية تساهم في تشجيع الإبداع

تعد برامج العصف الذهني والخرائط الذهنية من أمثلة الحلول التقنية التي تساهم في تشجيع الإبداع. وتُعرّف عملية العصف الذهني بأنها نشاط منظم يهدف إلى التوصل لأكبر عدد من الأفكار من المشاركين بدون أن يتم تقييمها أو انتقادها، مما يكون له الأثر الأكبر في إعطائهم الحرية لإطلاق العنان لإبداعاتهم وأفكارهم.

أما الخرائط الذهنية فهي وسيلة فعّالة وسهلة جدا لتلخيص الأفكار المتعلقة بموضوع معين، قد تكون الخريطة الذهنية بسيطة يمكن رسمها باستخدام أوراق وأقلام ملونة و يمكن تطويرها باستخدام برامج حاسوبية متخصصة. يوضح الشكل (٣) خريطة ذهنية مختصرة لنشاطات القسم النسائي المتعلقة بتنظيم المؤتمر السعودي الدولي الثاني لتقنية الإلكترونيات والاتصالات والضوئيات. وقد استخدم لتطوير هذه الخريطة موقع بوبل الذي يتيح العمل على تطوير الخريطة الذهنية مجاناً عبر الويب.

يلخص الجدول (١) أهم البرامج المجانية المستخدمة للعصف الذهني وتصميم الخرائط الذهنية التي تدعم معظمها باستخدام اللغة العربية، ولاختيار البرنامج المناسب للتطبيق يجب الأخذ بعين الاعتبار المعايير الآتية:

- دعم اللغة العربية
- إمكانية العمل المشترك من حيث تصميم الخرائط و تعديلها و خاصية إدارة المشاريع.

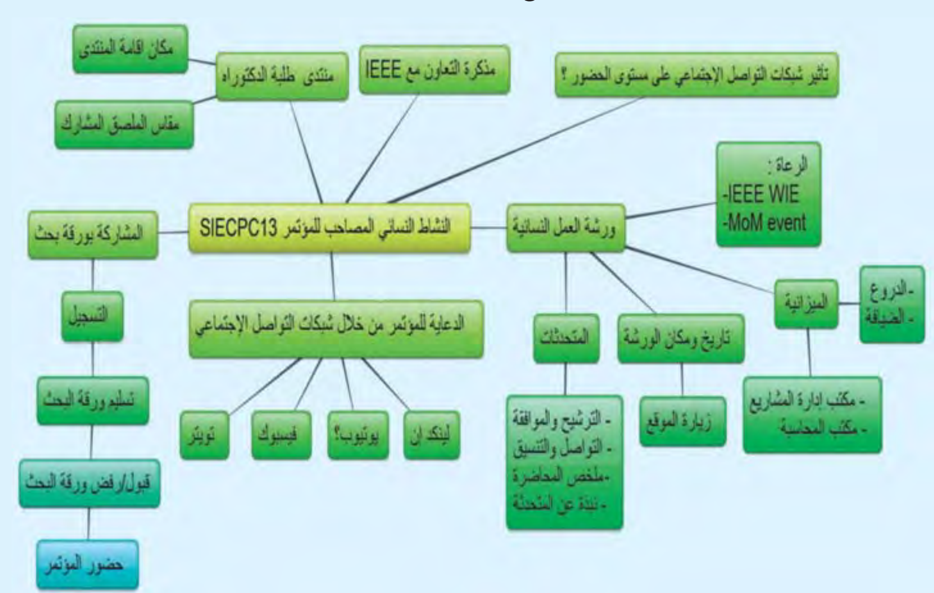
البرنامج	الموقع الإلكتروني
بوبل	Bubbl.us
مايندومو	www.mindomo.com
إكس مايند	www.xmind.net
سبايدر سكرايب	www.spiderscribe.net
مايند ميستر	www.mindmeister.com
وايز مابينق	www.wisemapping.com

■ جدول (١) أمثلة لبرامج العصف الذهني والخرائط الذهنية المجانية.

- عمل البرنامج عبر الويب أو الحاجة لتنزيل نسخة على سطح المكتب.
- أي احتياطات أمنية مهمة من حيث حماية المحتوى و سرية المعلومات.
- دعم البرنامج لنظام التشغيل المستخدم في المنشأة.

خاتمة

لا يختلف اثنان على أهمية بناء بيئة عمل تشجع على طرح الأفكار الجديدة لا سيما في المنشآت التي يشكل الإبداع أساس عملها كما هو الحال في المراكز البحثية؛ لذلك يجب أن لاتُغفل الخطوات المهمة المتبعة لخلق منظومة متكاملة لتشجيع توليد الأفكار و تطبيقها. فمن وجهة نظر إدارية و تنظيمية يجب أن تكون الخطوة الأولى عمل تقييم شامل ومتكامل لوضع المنشأة، يلي ذلك وضع خطة مدروسة لتشجيع الإبداع بالشكل الذي يخدم الأهداف الإستراتيجية الأساسية. وعند وضع مثل هذه الخطة يجب أن لا يُغفل دور التقنية في المساهمة بشكل فعّال في تشجيع الابتكار، وإمكانية الاستفادة من تجارب الدول المتقدمة والتي تميزت في هذا المجال مثل: اليابان وأستراليا والولايات المتحدة الأمريكية.



■ شكل (٣) خريطة ذهنية مبدئية لنشاطات القسم النسائي بمركز الإلكترونيات والاتصالات والضوئيات المتعلقة بتنظيم المؤتمر السعودي الدولي الثاني لتقنية الإلكترونيات والاتصالات والضوئيات.

المراجع

- **أحمد بوشنافة و طارق حمول**، إدارة الأفكار والمساهمة في الابتكار داخل المنظمات الاقتصادية الجزائرية، معهد العلوم التجارية والاقتصادية، الجزائر. ٢٠١٠م.
- **بندر الضبعان**، كيف نوفر بيئة عمل .. محفزة للإبداع؟، صحيفة الإقتصادية، ٢-٧-٢٠١٢م.
- **عبد الرحمن عدس**، الإبداع والشخصية، دراسة سيكولوجية، دار المعارف، مصر، ١٩٩٩م.
- **فتحي جروان**، الإبداع، دار عمان للطباعة والتوزيع والنشر، الأردن. ٢٠٠٢م.

-Baumgartner, Jeffrey. An Introduction to Idea Management. 2008.

-Eggers WD and Singh SK (2009). The public innovator's playbook: nurturing bold ideas in government, Deloitte Research.

-Haley January Eckels, "How Google has created a culture of innovation" 05/21/2008.

-Mackinnon, Lauchlan. "How to Choose an Idea Management System." 2012. Idea Managment Blog.

-Naiman, Linda. "Fostering Creativity in the Workplace." 2010.

-Shrivathsan, Michael. "8 Idea Management Software Tools." 2012. Practical Innovation Management.

عرض كتاب

الإلكترونيات والاتصالات لغير المختصين

يعد هذا الكتاب أحد سلسلة كتب التقنيات الاستراتيجية المتقدمة بالمملكة العربية السعودية المنبثقة عن الخطة الوطنية للعلوم والتقنية والابتكار التي تنفذها مدينة عبد العزيز للعلوم والتقنية دعماً لمبادرة الملك عبدالله للمحتوى العربي.

صدرت الطبعة الأولى من هذا الكتاب باللغة الإنجليزية عام ٢٠٠١ م، وألفه **مارتن بلونوس (Plonus, Martin)**، وترجمه للغة العربية **د. حاتم النجدي**، وقام بمراجعته كل من **د. محمد عبد الستار الشيخلي و د. محمد عباسي**، وصدرت طبعته المترجمة إلى العربية عن المنظمة العربية للترجمة عام ٢٠١٢م.

جاء الكتاب في ٦٨٨ صفحة من القطع المتوسط مقسمة إلى تسعة فصول، وتقديم لمعالي رئيس **مدينة الملك عبد العزيز للعلوم والتقنية**، و مسائل، والثبت التعريفي، وثبت المصطلحات عربي – انجليزي، وإنجليزي – عربي، وفهرس الكتاب.

تطرق الكتاب في **فصله الأول** إلى أسس الدارات، مشيراً إلى تعامل الإلكترونيات مع التأثيرات المتبادلة بين الجهود والتيارات ضمن شبكة من المقاومات والملفات ذات التحريض و المكثفات، وذلك إما لتضخيم الإشارات أو لتوليدها بشكل معين وبالتالي دارسة الإلكترونيات و المقاومات والملفات والمكثفات وهو ما يعرف بنظرية الدارات (Circuit Theory).

عرج المؤلف بعد ذلك إلى دراسة أساسيات الترانزستور الذي يقوم بعمل المضخم أو مبدال فصل و وصل، ومن ثم دراسة تصميم الدارات

أ. خالد بن عيد المطيري

الإلكترونية بما فيها من عناصر نشطة وغير نشطة والتي تكون تجهيزات مفيدة مثل أجهزة الراديو والتلفاز والحاسبات وغيرها.

تطرق المؤلف أيضاً إلى دراسة و تحليل دارات التيار المستمر (DC) ودارات التيار المتناوب (AC)، كما شرح هذا الفصل عدة مفاهيم أساسية مهمة في فهم الدوائر الالكترونية، حيث بدأ بالحقل الكهربائي التي تولده كل شحنة حولها ثم الجهد وهو العمل المبذول لوحدة الشحنة، فالتيار الذي يعرف بأنه المعدل الزمني لانتقال شحنة (Q) عبر نقطة مرجعية معينة، والاستطاعة وهي معدل القيام بعمل. ثم تطرق الكتاب في هذا الفصل إلى عدة قوانين مهمة وهي قانون أوم وقانون جول الحراري وقانون **كيرشوف**.

انتقل المؤلف بعد ذلك إلى توضيح عناصر الدارة الإلكترونية مثل: المقاومات، والمكثفات و الملفات (المحثات) والبطاريات، ومنابع الجهد والتيار، بالإضافة إلى تكافؤ المنابع والتحويل فيما بينها، مشيراً إلى أن هناك نوعان للدارات من حيث توزيع المقاومات بها وهما: دارة تسلسلية و دارة تفرعية، حيث قدم المؤلف شرحاً لكل منهما مع التوضيح بالرسوم والأشكال مع تقديم مثال لكيفية حساب المقاومة المكافئة في كلا الحالتين، كما أشار المؤلف إلى أنه يمكن تبسيط بعض الدارات باستخدام قواعد الدارات التسلسلية والتفرعية، ولكن في حال تبسيط دارات أكثر تعقيداً (شبكات) فثمة أدوات تحليل أخرى أكثر تطوراً ينبغي دراستها لتبسيط تلك الدارات، مشيراً إلى أنه في الإلكترونيات غالباً ما تواجهنا تجهيزات إما أحادية المنفذ (One port) أو ثنائية المنفذ (Two port) حيث تعد الثانية على قدر كبير من الأهمية لأن معظم التجهيزات الإلكترونية المعقدة تنتمي إلى هذه الفئة،

ثم تطرق المؤلف إلى مناقشة نظرية التراكب مشيراً إلى أنها تقوم على التحليل الخطي حيث أن علاقات الجهد والتيار الخاصة بالمقاومات والملفات والمكثفات هي علاقات خطية ينجم عنها مبدأ التراكب، ذاكرًا مثالاً على استخدام مبدأ التراكب لحساب التيار الكهربائي.

كما تطرق المؤلف إلى مبرهنة **ثفينين (Thevinin)** وأنها إحدى أقوى مبرهنات نظرية الدارات وأكثرها فائدة، فهي تسهل تحليل كثير من الدارات الخطية وتُعطي فكرة عن سلوكها، مشيرًا إلى أن مبرهنة **ثفينين** تكملها مبرهنة **نورتون (Norton theorem)** التي تنص على أن الدارة المكافئة للمنفذ الأحادي يمكن أن تكون منبع تيار حقيقياً أيضاً.

تناول **الفصل الثاني** من الكتاب دارات التيار المتناوب من خلال عدة موضوعات بدأها بتقديم تطرق فيه إلى أن أبسط الجهود والتيارات المتغيرة مع الزمن التي تصادفنا في الدارات على نطاق واسع هي الجهود والتيارات الجيبية (Sinusoidal) حيث أنها تبدل اتجاهاتها دورياً وتعرف عموماً بالتيارات المتناوبة. تلا ذلك موضوع التوابع الجيبية حيث يتم حساب الجهد الجيبي في دارة تسلسلية بواسطة تطبيق التحليل الشعاعي الطوري (Phasor analysis)، وهو شعاع يشتق من شعاع دوار يسمى المقدار

الموجود بين حاصرتين ممانعة، وتستخدم في تحليل التيار المتناوب مع ملاحظة أن الممانعة هو مقدار عقدي، وفي الواقع يمكن القول إن تحليل دارات التيار المتناوب هو تحليل دارات تيار مستمر باستعمال مقادير عقدية إلى جانب أن الممانعة تستعمل غالباً القبولية والتي تعرف بأنها مقلوب الممانعة.

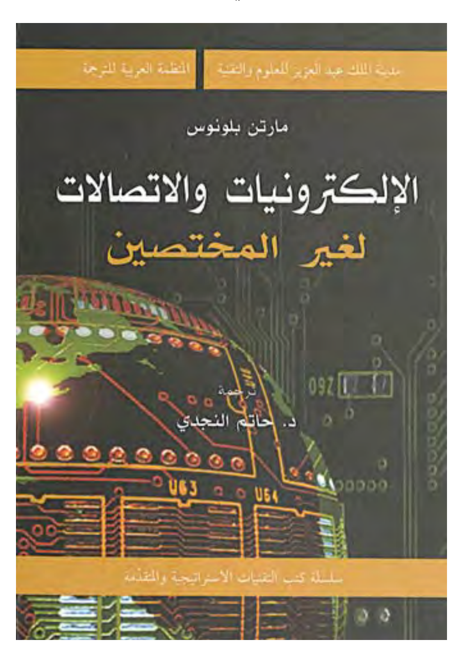
تطرق المؤلف في هذا الفصل أيضاً إلى المرشحات التي تستخدم لتمرير الترددات سواءً كانت عالية أم منخفضة، وذكر أمثلة لمرشحات بسيطة مكونة من عنصرين وشائعة الاستعمال وهي: مرشح (RC) ومرشح (RL)، مشيراً إلى أن مرشحات (RC) هي المفضلة علمياً لأنها أقل تكلفة. تستخدم مرشحات تمرير الحزمة في التوليف لانتقاء محطة أو قناة إذاعية أو تلفزية من بين عدد كبير من القنوات، فعلى سبيل المثال تقع قنوات التلفاز ٢-٦ ذات الترددات العالية جداً ضمن الحزمة الترددية من ٥٤ إلى ٨٨ ميجا هرتز وتحتل كل قناة حزمة ترددية عرضها ٦ ميجا هرتز. ولاستقبال قناة معينة، فإنه يستعمل مرشح تمرير حزمة ترددية يسمح لتردداتها بالمرور ويمنع مرور ترددات القنوات الأخرى، موضحاً أن أبسط مرشحات تمرير الحزمة هي الدارات الطنينية.

استعرض المؤلف أنواع الدارات مشيراً إلى أنهما نوعان هما: دارات التيار المتناوب التي تُغذى بجهد جيبي تردده يساوي ٦٠ هرتز، والدارات الراديوية وتُغذى بجهد جيبي تردداته من ١٠٠ كيلو هرتز حتى ١ جيجا هرتز.

ختم المؤلف هذا الفصل بتناول المحولات وموافقة الممانعة حيث تستعمل المحولات لنقل استطاعة الجهد المتناوب، أو لتغيير الجهود أو التيارات المتناوبة إلى قيم أعلى أو أقل، وتعد المحولات تجهيزات وحيدة التردد (٦٠ هرتز في شمال أمريكا مثلاً)، وذات مردود يقارب الـ ١٠٠٪.

ناقش **الفصل الثالث** تطبيقات الدايود (Diode)، حيث أوضح المؤلف أن الدايود يعد عنصراً لا خطياً ذو نهايتين أو قطبين وهو أقرب إلى مبدال الفصل والوصل، فعندما يكون في حالة وصل يعمل كدارة القصر ويمرر التيار. أما عندما يكون في حالة الفصل فإنه يعمل كالدارة المفتوحة ولا يسمح لأي تيار بالمرور. ثم تطرق المؤلف إلى التقويم حيث صنّفه إلى نوعين من المقومات وهما: مقوم نصف الموجة، ومقوم الموجة الكاملة، بالإضافة إلى المرشحات التي تستخدم لتمرير الترددات المنخفضة. موضحاً أن مرشح المكثفة يؤدي دوراً عظيماً في تكوين الجهد المستمر ولكن بعد تنعيم الموجة النبضية.

انتقل المؤلف للحديث عن دارات القص والقمط، حيث ذكر أن الوظيفة الشائعة لدارة القص هي قص جزء من إشارة الدخل، ويمكن استعمالها للحماية من زيادات الجهد الطارئة، و لتحديد الضجيج التي يمكن أن يعترض إشارة



مختارة في مستقبل راديوي. وفي موضوع تنظيم الجهد بدايود زنر، تم وصف استخدام دايودات زنر (Zener) لجعل الجهد في بعض الدارات الإلكترونية مستقرة، وهو نوع من الدايودات التي يمكن أن يتعافى من الانهيار الذي يحدث عند تجاوز الجهد العكسي.

استعرض المؤلف المقومات المتحكم فيها بالسليكون حيث أشار إلى أنها تعد من من التجهيزات ذات التطبيقات الواسعة في الصناعة، فهي تستعمل للتحكم السريع في المحركات، وفي شدة الإضاءة، وفي حرارة الأفران. كما تستعمل لتقويم التيار المتناوب وجعله مستمراً، مما يعد أحد أهم استعمالات الدايودات. لذا تحتوي كل التجهيزات الالكترونية على وحدة تغذية تقوم بهذه المهمة إضافة إلى ترشيح الجهد المقوم لجعله ناعماً ومستقراً.

تناول **الفصل الرابع** الدايودات والترنزستورات نصف الناقلة حيث بدأ الفصل بتقديم أشار فيه المؤلف إلى أن الدايودات نصف الناقلة هي وصلة بين مادتين نصف ناقلتين إحداهما من النوع الموجب والثانية من النوع السالب، لذا يعدُ فهم هذه الوصل مهماً في فهم الدايودات والترانزستورات. انتقل المؤلف للحديث عن نقل التيار بالثقوب والإلكترونات في أنصاف النواقل حيث أوضح أن الثقوب في نصف الناقل المشوب (Extrinsic) بالنوع (P) هي الحوامل الأكثر استخداماً، وأن النقل الكهربائي يحصل بالإلكترونات وحوامل الشحنة الموجبة التي تسمى ثقوباً والتي ينشأ الواحد منها عندما ينكسر رابط ويتحرر إلكترون (وهي ظاهرة تسمى عادةً بتكوين زوج الثقب والإلكترون)، كما تطرق المؤلف إلى أنواع أنصاف النواقل والناقلية في النواقل المشوبة إضافة إلى وصلة نصف الناقل والدايود والذي تطرق للعديد

من الموضوعات مثل: الانحياز الأمامي والعكسي ومعادلة المقوم، وطريقة التقريب لتحديد نقطة العمل، وانحياز الترانزستورات (MOSFET)، وانخفاض الربح بسبب مقاومة الانحياز، واعتبارات الأمان والتأريض.

كما ناقش المؤلف موضوع الوصلة (pn) والترانزستور من خلال عدة موضوعات فرعية وهي الترانزستور، والوصلة ثنائية القطبين، وترانزستور المفعول الحلقي، وخصائص التحويل، والمضخم الترانزستوري، وعناصر المضخم، وتصميم الانحياز الذاتي، والانحياز بتيار ثابت، والطريقة البيانية.

اختتم المؤلف هذا الفصل باستعراض مفعول التضخيم بيانياً باستخراج معادلة خط الحمل أولاً، ثم رسمها فوق خصائص خرج الترانزستورز وبعد اختيار نقطة العمل على خط الحمل، وتصميم دارة الانحياز للحديث عن ذات الجهد المستمر التي تحقق نقطة العمل تلك.

خصص المؤلف **الفصل الخامس** للحديث عن دارات المضخمات العملية، حيث بدأ بمقدمة استعرض خلالها خصائص المضخم المثالي التي تستخدم غالباً بوصفها أهدافاً تصميمية لمضخمات عملية، ومن ثم تناول موضوعات فرعية مثل مضخات الإشارات الصغيرة، وتقدير الربح بالديسيبل، واستجابة المضخم الترددية، والاستجابة الزمنية ومضخات النبضات، ومضخمات الاستطاعة. بين المؤلف أنه كلما كانت تغيرات الإشارة أسرع، وجب أن يكون عرض حزمة المضخم أكبر لتحقيق تضخيم للإشارة بدون تشويهها، بعد تحقيق تضخيم كاف لجهد الإشارة، وهو غالباً الهدف النهائي في بعض التطبيقات، يمكن زيادة استطاعتها أيضاً. ويتحقق ذلك بإدخال الإشارة المضخَّمة إلى مضخم استطاعة.

اختتم المؤلف هذا الفصل بذكر المستقبل الراديوي ذو التعديل المطالي (Amplitude modulation) والذي يعد مثالاً لجمع مكونات تبدو شديدة التباين ضمن منظومة عملية، إلا أنه يمكن لمستقبِل التعديل الترددي أو لمستقبل التلفاز أو غيرها من التجهيزات الإلكترونية أن تكون مثالاً أيضاً. وبالرغم من أن كثيراً من مكونات المستقبِل تصنع على شكل رقاقات، إلا أن مخطط عناصر المستقبِل المنفصلة مكّنت من دراسة مبدأ المزج الترددي وفك التعديل والتحكم الآلي بالربح.

استعرض المؤلف في **الفصل السادس** مضخمات العمليات من خلال عدة موضوعات حيث تطرق المؤلف في مقدمة الفصل إلى التعريف بأن المضخمات عبارة عن دارة متكاملة عالية الربح مكونة من نحو عشرين ترانزستور ذات ربط مباشر فيما بينها، ثم تناول عدة موضوعات أخرى متعلقة بمضخات العمليات مثل مضخم العمليات والمضخم المثالي الذي تم تقسيمه إلى مضخم معاكس وغير معاكس، وتوابع الجهد والحائل الواحدي الرابح، والجوامع والطوارح، والمبدلات الرقمية التماثلية، والمضخم التفاضلي واستخدامه في التطبيقات والقياسات الحيوية الطبية، ومضخمات التفاضل والتكامل واللوغاريثم والمرشحات الفعالة ، والمقارن والمبادل التماثلي الرقمي، والحاسوب التماثلي.

ناقش **الفصل السابع** الإلكترونيات الرقمية، وبدأ بمقدمة تساءل فيها عن سبب الاهتمام بالعالم الرقمي وكانت الإجابة هي وجود الحواسيب الرقمية ومناعة نقل المعلومات الرقمية تجاه الضجيج، فالحواسيب مستمرة في تزايد أهميتها بوصفها معالجات رقمية، وهي متزايدة الأهمية أيضاً بوصفها منابع جديدة للمعلومات الرقمية. وثمة حاجة إلى المعرفة الأولية بالإلكترونيات الرقمية بغية مواكبة التطورات السريعة في مجال الهندسة التي تهيمن عليه باطراد كل أنواع الدارات الرقمية، لا الحاسب فقط.

بعد ذلك تطرق المؤلف للعديد من الموضوعات مثل: تمثيل الإشارة الرقمية، والمنطق التجميعي، ودارات المنطق التجميعي، ودارات المنطق المتسلسل، والعدادات الرقمية، والذاكرة.

تطرق المؤلف في **الفصل الثامن** إلى الحاسب الرقمي، حيث بدأ الفصل بمقدمة تطرق فيها إلى أن تطبيقات الحاسب الرقمي وشبكات الاتصالات الرقمية - التي أتت بعده - من أهم التطورات التقنية اللافتة التي حدثت، ونظراً إلى أن هذين المجالين يشتركان في نفس لغة الثنائي، فقد اندمجا وتطورا معطين نتائج ثورية تجلت في شبكة الانترنت وشبكة الوب العالمية، وغيرت ثورة المعلومات المسماة بالثورة الثالثة، كما تناول الفصل العديد من الموضوعات الأخرى مثل: قوة الحاسب، وعناصر الحاسب، ووحدة المعالجة المركزية، والأعداد الستة عشرية وعنونة الذاكرة، ونظم التشغيل.

تناول **الفصل التاسع** والأخير المنظومات الرقمية حيث بدأ بمقدمة تناول فيها أثر اختراع الترانزستور على صناعة الإلكترونيات كما ناقش العديد من الموضوعات الأخرى مثل : الاتصالات الرقمية والحاسب، والمعلومات، ومعدل المعلومات، وشبكات الاتصالات الرقمية.

يعد هذا الكتاب من الكتب الشاملة والحديثة في مجال الإلكترونيات والاتصالات، حيث أنه قدّم العديد من المفاهيم والموضوعات والتعريفات والنظريات والمعلومات المفيدة التى تُفيد العديد من القارئين المهتمين بهذا المجال؛ ويمثل الكتاب إضافة جديدة وجيدة للمكتبة العربية.

تحت رعـاية خـــادم الحرمـــين الشريـــفين
الملك عبدالله بن عبدالعزيز آل سعود



المنتدى الرابع للبتروكيماويات ٢٠١٤

بين مدينة الملك عبدالعزيز للعلوم والتقنية وجامعة أكسفورد

٢٧-٢٨ رجب ١٤٣٥هـ الموافق ٢٦-٢٧ مايو ٢٠١٤م

مقر المدينة الرئيس، قاعة المؤتمرات، مبنى ٣٦، طريق الملك عبدالله، الرياض



www.kacst.edu.sa

كيف تعمل الأشياء؟

الـــرّادار

أ. محمد صالح سنبل



الـرّادار (الـرّاصـد) جهازٌ يتكوّن مـن وَحْـدات ودوائــرَ إلـكترونيّة وميكانيكيّة تعمل معًا في تزامن دقيق جدًا، عبر إرسـال واستقبال نبضات من المَوْجَات الكهرومغناطيسيَة المُرْسلة والمستقبلة من هوائيات موجهة. سُمِّي الـرّادار (Radar) بهذا الاسم اختصارًا لأربع كلمات باللغة الإنجليزيّة، هي (Radio Detection And Ranging). يَسْتَخْدم الرّادارُ مَوْجات الرّاديو؛ وذلك بقصد كَشْف ارتفاع العديد من الأجسام الثابتة أو المتحرِّكة ومسافتها وسرعتها وتعقّبها ، مثل: الطّائرات، والصّواريخ، والعرَبات، وغيرها. كما يُسْتَخْدَم للكَشْفِ عن الأحوالِ المُناخيّة ورَصْدِها.

يَعُـود ابتكارُ الـرّادارِ إلى بدايات القـرْنِ المُنْصَرِم؛ إذ اسـتخدمه العـالمُ الألمـانيّ **كريستيان هولسماير** عام ١٩٠٤م ؛ للكشـف عن إحدى السّـفن المُبْحِرَة وسط الضّبـاب، وقُبَيْلَ الحرب العالميّة الثانيّـة اسْتَخْدَمَ عالمُ الفيزيـاء **نيكولا تيسلا** عـام ١٩١٧م الـرّادارَ البدائيّ مُعْتَمِدًا علـى أُسُس علم الكهرباء فيمـا يَتَعَلَّق بالمَوْجات ومستويـات الطاقـة، وفي العـام ١٩٢٢م وَصَـفَ العـالم **ماركوني** أساسيّات عمل الرادار وقدّمها، وتوالى تطوير أنظمة الرادارات حتّى ظهر أوّل رادار مُتَكامِل حديث في عـام ١٩٣٥م في بريطانيا. تلا ذلك استخدام أوّل رادار بحريّ على متن السّفن الحربيّة في عام ١٩٣٧م، وبعدها بِسَبْع سنَوات اُسْتُخْدِمَ الرّادار البحريّ على متن السّفن التجاريّـة؛ لتحديد المَواقع والأهـداف الثابتة والمتحرِّكة



■ الرّادار البحريّ.

حولَ السفينة، واستمرّ تطوير الرّادارات بعد ذلك؛ لتزويدهـا بأنظمة دفاعيّة؛ لاستخدامها في مُختلف المجـالات البحثيّـة المُتَنَوِّعَـة، مثل أبحـاث الفضاء والفلك والأرصاد الجوّيّة.

مُكَوِّنـات الـرّادار

يتكوّن الرّادار من أربع وحدات رئيسة هي:

● **وحدة الإرسال**

تولِّدُ وحـدة الإرسـال (Transmitter Unit) الإشـارات اللاسلكيّةَ (النّبَضـات الرّاداريّة) التي تمتلـك طاقـةً كهرومغناطيسيّـةً عالية جـدًّا ثابتة الـتّردّد إلى الخـارج عَبْرَ أنبوبـة تَوْجيـه المَوْجات، كمـا تنتقلُ هذه النّبضات على هيئة مَجالٍ كهربائيّ ومغناطيسـيّ متعامِدَيْن على بعضهمـا بعضًا، ويتمّ ذلـك بوساطـة أنبوبـة مُسْتَطيلـة الشـكل نُحاسِيَّة القوام مُفْرَغَة من الداخل.

تتكوّن وحـدةُ الإرسال من ثلاث وحدات رئيسة تتكامل في مُهِمّتها، وهي:

■ **المُؤَقّت** (The Trigger Generator): وتُنْتِـجُ نبضـةً كهربائيّة – لهـا فرقُ جهـد مُنخفِض– على صـورة مَوْجات مُدَبَّبَة إلى وحدة المُعَدَّل، كما تتحكّم هذه الوحدة في المُعَدَّل التَّكراريّ للنّبْضة.

■ **المُعَـدِّل** (The Modulator): وتتحكّـم في مـدّة النبضــة المُرْسَلــة وشكلهـا وطاقتها، كمـا تعمل على تحويل التّيارات إلى نبضات ذات طاقة مُرْتَفِعَة جدًّا.

■ **المجنيترون** (The Magnetron): وتَرْفَعُ تردّد النّبضـات وتُحَوِّلُهـا إلى نبضـات كهرومغناطيسيّة تسـري عـبر أنابيب التوجيـه، عن طريـق الهوائيّ المُوَجَّه باتّجاه الفضاء الخارجيّ.

● **وحدة الاستقبال**

تستقبل وحـدة الاستقبال (Receiver Unit) الأصداءَ المُرْتَـدَّة من الأجْسَام الثّابتـة أو المتحرّكة المُجـاوِرَة للـرادار؛ لإظهارهـا علـى شاشتـه، كما تُضَخِّـم (تُكَـبِّر) هذه الوحـدة الأَصْـداءَ الضّعيفةَ المُرْتَـدَّة، التـي تُسْتَقْبَـل عـبرَ الهوائـي، ثـم تُهَيِّئَ معلومات بالقيمـة المُناسِبَة، والصورة المطلوبة التي تظهر على شاشة الرّادار.

تتكوّن وَحدَةُ الاستقبال من عدّة وحدات، هي:

- المُذَبْذب المَحَلّيّ (Local Oscillator).
- الخَلّاط (Mixer).
- التّوليف (Tunning).
- التّكبير (I.F. Amplifier).
- المُحَدِّد (Detector).
- تكبير النّبضة المَرْئيّة (Video amplifier).

● **وحدة الهَوائيّ**

تُرْسِـلُ وحـدة الهوائيّ (Aerial Unit) الطّاقـة (النّبضـة) الرّاداريّة على صـورة نَبَضاتٍ قويّـة وقصـيرة الطـول المَوْجـيّ، وذلـك في جميع الاتّجاهـات؛ تمهيدًا لاستقبال الصّـدى العائد من الأهداف المُراد تَعقّبُها؛ إذ يدور الهوائيّ حول نفسه بسرعة؛ لإرسال الطاقة واستقبالها من الاتّجاهات جميعهـا، ويُصَمَّـم الهوائـيُّ بحيـث يـوزّع الطّاقة الرّاداريّـة علـى صـورة حُزْمـةٍ مَعلومـةِ الارتفـاع الرّأسيّ، والعَرْض الأفقيّ.

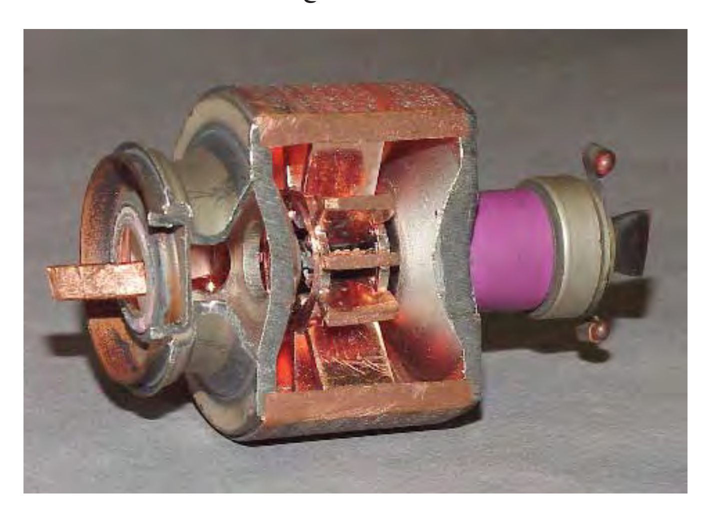
يتكوّن الهوائيّ من ثلاثة عناصرَ رئيسة، هي:

■ **أنبوبـة توجيـه النّبضـات** (Wave Guide): وهـي دائريّـة أو مُسْتَطيلـة الشـكل، مَصْنوعَة من النّحاس، وتَعْبُرُ فيها الطّاقة عالية التردّد من وحدة المجنيترون إلى وحدة الهوائـيّ، عبر وصلة خاصّة، لها القدرة على الدَّوَران مع الهوائيّ؛ بقصد إيصال الطاقة إلى مركز الهوائيّ.

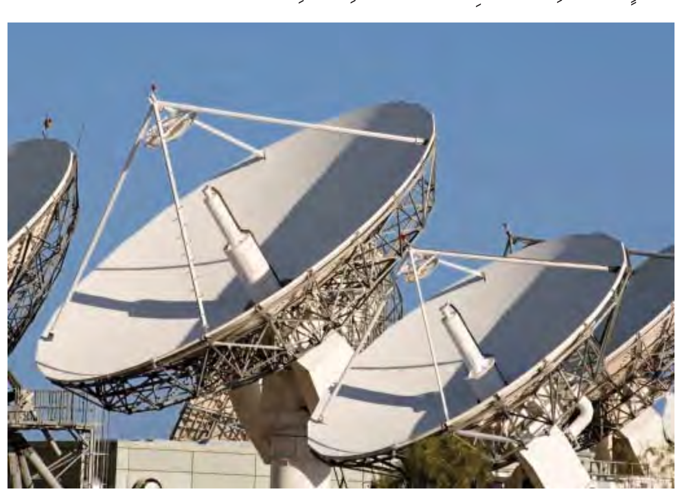
■ **إرْسال واسْتِقْبال** (Trlrx Switch): وتتمثّـل مُهِمَّتُهـا في السّمـاح بمـرور الطّاقـة المُرْسَلَـة مـن المُرْسِـل إلى الهوائيّ بدون الحاجة إلى الوصول إلى المُسْتَقْبِـل، بواسطـة أنبوبة توجيـه النّبضات؛ مما يسمح بإطلاق أكبر كمّيّة من الطّاقة؛ لِبَثّ المَوْجات المُرْسَلـة. أمّا الاستقبال فعندمـا يرتدّ الصّدى من الأجسام المُـرَاد تعقّبُها؛ فإنّه يكون ضعيفًا، ويحتاج إلى تكبـير، فيَتَّجِـه إلى أنبوبة توجيـه النّبضاتِ في اتّجاه المستقبل، دون المرور على المُرْسِل.

■ **الهَوائـيّ** (Scanner): ويُوَجِّه الطّاقة الرّاداريّة تجـاهَ مَسـارٍ مُحَـدَّد؛ لتحديد الاتّجـاه النّسْبِـيّ أو الحقيقـيّ للأصـداء المُرْتَدَّة من الأهـداف، ويوجد نوعان من الهوائيّات، هما:

- **الهَوائـيّ المُقَعَّر** (The Parabolic Reflector): وهـو لـوحٌ مَعْدنيّ، لـه شكل قطـع مكافـئ، يَنْشُر الطّاقـة الرّاداريـة علـى هيئـة خطـوط متوازيـة، وتنطلق النّبْضة الرّادارية من أنبوبة مَرْكزيّة تُسَمَّى البـوقَ، وذلـك باتّجاه القطـع المكافـئ. يمتاز هذا الهوائـي برُخْصِ ثمنـه، إلّا أنّه يُعـابُ عليه حَجْمُه



■ وحدة المجنيترون.



■ وحدة الهوائي تقع في منتصف الرادار، وهي أسطوانية الشكل ومستقيمة.



■ وحدة عرض المعلومات الرادارية.

■ انبعاث وارتداد موجات الرادار.

ووزنُه الكبيران، إضافة إلى تأثّره بالرّياح.

- **الهَوائيّ ذو الأنبوبة المُثقّبة** (Slotted Wave Guide): وهو ذو أنبوبة توجيه مثقوبة، أحد طَرَفَيْها مفتوحٌ والآخرُ مُغلَق، ويُثبَّتُ حولَها صندوقٌ من مادّة الفايبرجلاس للحماية، ويمتاز هذا الهوائيّ بحجمه الصّغير، وقلّة الطّاقة المفقودة، إضافة إلى تركيز الطّاقة في حُزَم ضيّقة، إلّا أنّه باهظُ التكلفة وعرضة للكسر.

● **وحدة عرض المعلومات**

تعمل وحدة عرض المعلومات (The display Unit) - بصورة أساسيّة - على تحديد وجود الأهداف؛ بإظهار الصّدى على شاشة صمّام أشعّة المهبط (الشّاشة الرّاداريّة). ويحدث ذلك عبر حدوث لَمَعانٍ للنّقطة المُضيئة مكانَ الصّدى الذي اُستُقْبِلَ؛ بحيث يمكن قياس كُلٍّ من مدى هذا الهدف واتّجاهه. وحتّى يمكن الحصول على الصّورة الرّاداريّة للهدف (الأهداف) المطلوب عرضُها؛ فإنّه يُدْخَل مجموعة من الإشارات إلى وحدة عرض المعلومات، هي:

١- إشارة المُؤقّت (Trigger).

٢- الأصداء العائدة من الأهداف بعد تضخيمها (The amplified echoes).

٣- إشارة التّزامن بين الهَوائيّ وخطّ الأساس الزّمنيّ (The rotation signal).

٤- إشارة علامة مُقَدِّم السّفينة (The heading marker signal)، وذلك في حالة رادارات السّفن.

كيفية عمل الـــرادار

تتمثّل طريقة عمل الرادار في بثّ وحدة الإرسال موجات الرّاديو المُكثّفة، لها أطوالٌ مَوْجيّة مُخْتلفة، تنتشر حول الرادار مدّةً زمنيّة مُعيّنة، على هيئة طاقة راداريّة، وهذه الموجات لها سرعةٌ تُقَارِبُ سرعةَ الضّوء (٣٠٠ م/ ميكرو ثانية). أما مَوْجات الرّاديو فهي مجال مغناطيسيّ، وآخرُ كهربائيّ متعامدان، ولهما نفس التردد والطول الموجيّ، ويَحْدُث بعدئذ انعكاسُ الصّدى؛ ففي حالة وجود أجسام في طريق الرّادار تعكس هذه الأجسام بعضَ الطّاقة الكهرومغناطيسيّة، أمّا موجات الراديو فيحدث أن تنعكس إلى الرّادار مجددًا، ويحدث الانعكاس من مُخْتَلف الزّوايا، كما هو الحال في لَمَعان كرة زجاجيّة.

يمكن - بوساطة مَعرفة سرعة الانتشار للمَوْجات الكهرومغناطيسيّة والمدّة الزمنيّة بين إرسال النّبَضات من وحدة الإرسال حتّى استقبال الصدى العائد منها -حسابُ المسافة التي قطعَتْها النّبضةُ الرّاداريةُ منذ إرسالها وحتّى استقبال صداها، وتصبح المُعادَلة كالآتي:

المَسافة المَقطوعة = المدّة الزمنيّة X سرعة انتشار المَوْجات.

يتأثّر الرّادارُ بالعديد من الظّروف الجوّيّة السّيّئة، كما يصدر من الرّادار العديدُ من أصوات الضّجيج، التي في الأساس منشؤها خارجيّ؛ بسبب صدى المَوْجَة اللاسلكيّة، التي تعود من هدف ليس ذو فائدة، مثل الأجسام الطبيعيّة: كالأشجار والصّخور والحيوانات، إضافة إلى بعض المُؤثّرات الأخرى، مثل: الغيوم والأعاصير والنيازك الصغيرة والمباني السكنيّة.

أهميّة الـــرّادار

هناك العديدُ من الفوائد والتطبيقات للرادار، منها :

١- تحديد مواقع الأجسام المتحرّكة، مثل: الطائرات والسفن والصواريخ والنيازك، وذلك في مُخْتَلف حالات الطّقس المتقلّبة نهارًا وليلًا.

٢- تزويد المتخصّصين بالمعلومات والإرشادات الملاحيّة في كافّة الأوقات، على مدار السّاعة.

٣- منع حدوث اصطدام الطّائرات في الجوّ والسّفن في المحيطات، إضافة إلى إرشادها وتوجيهها في خطّها الملاحيّ أثناء الأحوال الجوّيّة السّيّئة.

٤- رصد الأجرام السماوية القادمة إلى المجال الجوي الأرضي وتعقّبها.

٥- البحثُ عن مواقع حطام الطائرات والسفن المفقودة.

المراجع

- http://www.howstuffworks.com/-radar-detector١.htm

- http://www.q٨ship.com/qqq/radar.htm



مشـروع نظـام «مؤشـر»

يشهد العالم تطوراً مذهلاً في جميع المجالات خاصة مجال الإلكترونيات والاتصالات التي جعلت العالم قرية صغيرة يتفاعل أفرادها مع بعضهم البعض فكل جديد لا يلبث إلا أن ينتشر في أرجاء المعمورة بفضل تلك الطفرة الهائلة في هذه التقنيات، وإيماناً من مدينة الملك عبد العزيز للعلوم والتقنية بضرورة الإسهام في تطور هذا المجال فقد قامت بدعم مشروع بحثي تحت مسمى « مؤشر » وهو عبارة عن جهاز محمول خفيف الوزن يقوم بتتبع المستخدم ومعرفة الكثير من بياناته ثم إرسالها إلى مركز القيادة والتحكم ليتم عرضها على الخارطة . مع إمكانية حفظ النظام لآخر الإحداثيات في قاعدة البيانات لهذا الجهاز المستخدَم.

يمثل المشروع أهمية حيوية في مجال الاتصالات بالأقمار الاصطناعية ، وقد قام فريق هندسي في المركز الوطني للإلكترونيات والاتصالات والضوئيات التابع للمدينة بتصميم وتصنيع وبرمجة واختبار جميع أجزاء المشروع في مراحله المختلفة. وكان الباحث الرئيس للمشروع م/**علي بن طاهر الصامطي** ومعه عدداً من الباحثين ومساعديهم بالمركز بتفيذ المشروع منذ شهر شوال ١٤٣٤هـ واستغرق إنجازه قرابة ستة أشهر.

هدف المشروع

كان الهدف من المشروع هو ابتكار نظام إلكتروني متكامل يُمَكِّن مدير النظام من مراقبة مستخدميه ومعرفة معلوماتهم الحيوية والجغرافية.

مواصفات النظام

تتمثل مواصفات نظام مؤشر فيما يلي:

- تحديد موقع المستخدم ومراقبته عن طريق الاتصال بالأقمار الاصطناعية.
- إرسال المعلومات الحيوية للمستخدم وموقعه الجغرافي برسالة مشفرة إلى مركز المراقبة والتحكم.
- عرض مواقع أجهزة المستخدمين ومعلوماتهم الحيوية على الخريطة وتحديثها باستمرار.
- إمكانية إرسال رسالة نصية إلى مركز المراقبة والتحكم عبر الأقمار الاصطناعية.
- إمكانية تخزين آخر مائة حالة لكل مستخدم في قاعدة بيانات النظام.

القطاعات المستفيدة من النظام

من أهم القطاعات التي يمكن أن تستفيد من نظام مؤشر ما يلي:

- القطاعات العسكرية (تحديد العربات والجنود).
- القطاعات الصحية (المرضى، وكبار السن).
- القطاعات الخاصة والعامة.
- الكشافة وهواة الصيد والرحلات البرية .

مراحل نظام مؤشر

كعادة أي مشروع ناجح، فلا بُد له من مراحل مختلفة يمر بها حيث تستهدف كل مرحلة تطويراً مختلفاً للنظام وإضافة مزايا جديدة، ومن أهم خطوات تطوير أي مرحلة هي: التخطيط، والتصميم، وتجهيز الطاقم المنفذ، والتنفيذ، والاختبار.

تهدف المرحلة الأولى من المشروع – بشكل رئيسي– إلى تحديد موقع المستخدم عن طريق استخدام شبكة الأقمار الاصطناعية،ومن ثم إرسالها مع حالة المستخدم الصحية (نبضات القلب) عن طريق شبكة الجوال «GPRS» بواسطة شريحة البيانات.

تم تطوير المشروع – في المرحلة الثانية – ليقوم بنفس مهام المرحلة الأولى مع إرسال البيانات عن طريق الأقمار الاصطناعية، فضلاً عن إضافة لوحة مفاتيح لإتاحة كتابة رسالة لمدير النظام وشاشة لعرض المعلومات.

النتائج

تم الانتهاء من المرحلة الأولى والثانية من النظام وتم اختباره مع أحد القطاعات العسكرية، حيث أثبت نجاحه عند تجربته وإرسال رسائل إلى مركز المراقبة والتحكم، حيث استقبل مركز المراقبة الرسائل بالشكل الصحيح والمطلوب .

المراحل المستقبلية للمشروع

لازالت هناك عدة مراحل لتطوير المشروع تشتمل كل منها على إضافة حسّاس واحد فقط لضمان مدى قدرة الجهاز على العمل في كل مرحلة، كإضافة حسّاس لقياس درجة حرارة جسم المستخدم، وحسّاس البصمة للتعرف على مستخدم الجهاز، وأيضا حسّاس لحفظ التوازن (Gyroscope) .

مصطلحات علمية

غرفة عديمة الامتصاص
Anechoic Chamber
غرفة تُصّمم لامتصاص كافة انبعاثات الموجات الكهرومغناطيسية أو الصوتية.

هوائي Antenna
قطعة معدنية تستخدم لالتقاط وبث الإشارات اللاسلكية، وتحويل الموجات الكهرومغناطيسية إلى تيار كهربائي والعكس ، وتتفاوت أنوع الهوائيات من حيث الحجم وتكلفة التصنيع ومقاييس الكفاءة، وتستخدم في جميع الأنظمة والاتصالات اللاسلكية، وشبكات تبادل البيانات المحلية اللاسلكية، وأنظمة الرادار، وتلسكوبات استكشاف الفضاء، وغيرها.

تصوير خلفي للشريحة Backside Imaging
تقنية حديثة تتم باستخدام أشعة تحتوي على فوتونات عالية الطاقة وذلك لاكتشاف الهجمات التي قد تحدث على جهاز التشفير.

دفاعات وحدات المعالجة Circuit Board
أحد الإجراءات الدفاعية أثناء تطوير أجهزة التشفير؛ لتجنب الهجمات المتوقعة.

معامل الارتباط Correlation Factor
معامل تستخدم لمعرفة العلاقة بين متغيرين أو أكثر وقد تكون هذه العلاقة إما طردية أو عكسية.

تقنيات رقمية Digital Technologies
تطبيقات متطورة للحاسبات وأنظمة الاتصالات تقوم بنقل واسترجاع ومعالجة البيانات، وتستخدم في برمجيات الحاسبات والإلكترونيات وأشباه الموصلات .

بطاقة الواجهة الرئيسة
External Interface Card
بطاقة تقوم بتحويل البيانات الرقمية إلى إشارات تناظرية تمهيداً لإرسالها عن طريق شبكة الهاتف، كما تقوم بتحويل الإشارات التناظرية الداخلة للجهاز إلى بيانات رقمية مفهومة للوحدات الداخلية للجهاز.

خوارزمية جينية Genetic Algorithm
تقنية حديثة تصنّف كأحد البحوث العالمية الاستدلالية، وهي إحدى طرق الخوارزميات المتطورة.

أيونوسفير Ionosphere
الطبقة العليا من الغلاف الجوي، وتمتد من ارتفاع ٥٠ كم إلى أكثر من ١٠٠٠كم فوق سطح الأرض، ويحدث بها تأيّن للذرات؛ مما يؤدي إلى تشتت موجات الراديو التي تمر من خلالها.

خوارزمية تشفير البيانات الدولية
International Data Encryption Algorithm- IDEA
أحد خوارزميات التشفير العالمية الآمنة تم تطويرها في زيورخ بسويسرا، وتتميز بكبر حجم الكتلة الذي يبلغ ١٢٨ بت.

لوحة رئيسة Main Board
أداة التحكم الرئيسة لجهاز التشفير والمسؤولة عن التحكم والربط بين الوحدات الداخلية.

ألياف ضوئية Optical Fibers
ألياف رفيعة وشفافة تستخدم لنقل البيانات عبر الإنترنت بسرعات عالية بدلاً من الاسلاك النحاسية.

جهاز قياس قوة الإشارة Oscilloscope
جهاز يقيس ويحلل الإشارات الكهرومغناطيسية المنبثقة من جهاز التشفير .

مصفوفة الهوائيات المتوافقة في الطور
Phased Antenna Array
مجموعة من هوائيات متماثلة مفصولة عن بعضها البعض بمسافة ثابتة ومرتبة على شكل صف لتشكل هوائي واحد بحيث يتم توصيل جميع العناصر بجهاز الإرسال أو الاستقبال (عناصر نشطة).

هجمات فيزيائية وتخريبية
Physical & Invasive Attacks
هجمات تُغير من حالة وتصرف النظام ويبقي أثرها باقياً على جهاز التشفير كدليل على حدوثها، وتهدف بصفة أساس إلى معرفة تامة بتخطيط الوحدات الداخلية ووظائفها لاستخلاص المعلومات الحساسة منها.

وحدة تشفير Processors Encryptation
وحدة مسؤولة عن عمليات التشفير وإدارة المفاتيح، ويعتمد نوعها على حجم ووظيفة ونوع جهاز التشفير.

رادار Radar
نظام تعقب يمكنه التقاط ذبذبات موجات الراديو وتحديد مدى واتجاه وسرعة الأجسام الغريبة مثل: الطائرات والصواريخ والمركبات الطائرة، وتعقب حالة الطقس.

الهجمات الهجينة Semi-Invasive Attacks
مزيج بين الهجمات التخريبية وغير التخريبية، وقد ظهرت تقنيات حديثة تدعم وتساعد في تطوير واكتشاف مثل هذه الهجمات وأصبحت تشكل مجالاً خصباً للبحث، لأنها تمثل حلاً وسطياً من حيث: السعر، والوقت، والأداء.

مفتاح كهربائي Swicth
وحدة تستخدم في الشبكات الحاسوبية بحيث يتم ربطها بأجهزة أخرى بهدف التواصل ونقل البيانات.

تشفير متماثل Symmetric Cryptography
أحد أساليب التشفير المعتمدة على وجود مفتاح سري مشترك بين كل من المرسل والمستقبل، كي يتمكن كل منهما من تشفير وفك تشفير البيانات باستخدام نفس المفتاح.

نظام في شريحة System on Chip
مكون رئيس في معظم الهواتف المحمولة الذكية، وهو عبارة عن دائرة متكاملة تحتوي على كل مكونات الحاسب الآلي مدمجة في شريحة، كما تحتوي على دوائر رقمية وتناظرية ومختلطة وأحيانا موجات الراديو، وتعد حاسبات مصغرة لها القدرة على العمل على أنظمة تشغيل ويندوز أو لينيكس وغيرها.

هاتف Telephone
جهاز إرسال واستقبال موصل بأسلاك مع مقسم رئيسي يقوم بنقل الصوت بشكل فوري بين مكانين يصل بينهما خط هاتف عند كل طرف منهما.

تروبوسفير Troposphere
الطبقة الأولى من طبقات الغلاف الجوي ، وتحدث فيها تفاعلات الطقس والتقلبات الجوية والأمطار والأعاصير، نتيجة لوجود بخار الماء في هذه الطبقة.



البطاطس وقُوّة ضغط الهواء

تُعَدُّ البطاطس مِن أشْهَرِ الخَضراوات وأكثرِها انتشارًا على مستوى العالم، وتُسْتَخْدَم كثيرًا في حياتنا اليوميّة؛ إذ إنها ذات قيمة غذائية عالية، كما أنّها تُزْرَع في العديد من مناطق العالم. تنمو دَرنات البطاطس تحت الأرض، وتُشَكِّلُ – إلى جانب القمح والأرز والذرة – أهمّيّةً اقتصاديّةً للعديد من دُوَلِ العالم.

توجد البطاطس في بيوتنا بصورة دائمة، ويُمْكِن استخدامها ليس فقط للغذاء، بل لِعَمَلِ تَجْرِبة علميّة يسيرة وطريفة ولا تَحْتاج إلى جهْدٍ كبيرٍ، ولها مَدْلولٌ علميٌّ مُفيدٌ.

تُوَضِّح هذه التّجْربة تأثيرَ ضَغْطِ الهواء في اختراق الأنسجة الصُّلْبة.

الأدَوات

- درنة بطاطس، شكل (١).
- ماصّة طويلة (المُسْتخدَمة في المشروبات)، شكل (٢).
- طاوِلة خشبيّة.

طـريقـة العمل

١- إحضارُ درنة البطاطس، ووضعُها على الطّاوِلة.

٢- الإمْساكُ بالمَاصّة، ومُحاوَلَة إدخالِها في درنة البطاطس.شكل (٣).

٣- إعادةُ المُحاوَلة، وإمْساكُ الماصّة، معَ إحْكام إغلاقِ طَرَفِها؛ لِمَنْعِ دخولِ الهواء، شكل (٤).

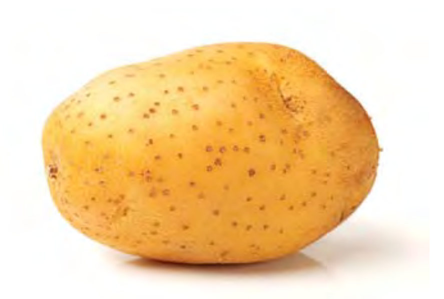
المـــلاحظة

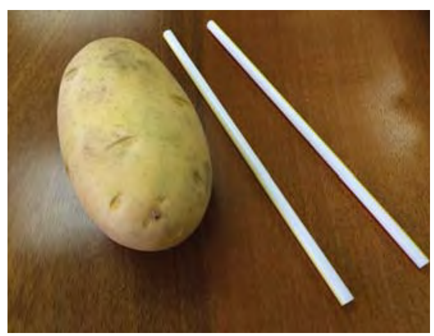
في المرّة الأولى عند الإمساك بالماصّة دون إغلاق طَرَفِها لوحِظَ عدمُ اختراقها لدرنة البطاطس؛ أمّا عندما أُحْكِمَ إغلاقُ طَرَفِ الماصّة؛ فقد تم إختراق الدرنة بنجاح.

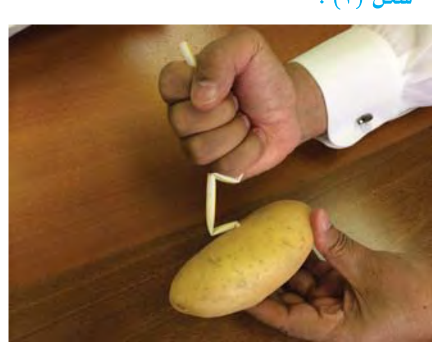
الاستنتـــاج

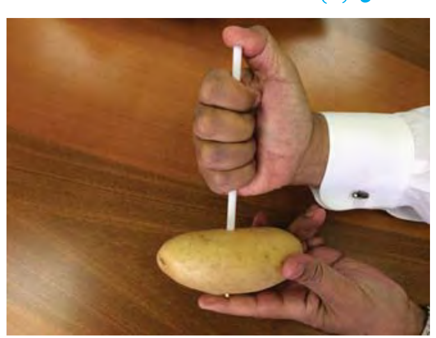
في المرّة الأولى لم يَحْدُثْ اختراقٌ لدرنة البطاطس؛ بسبب أنّ ضغطَ الهواء في داخل الماصّة لا يَسْمَح باختراقها، أمّا عندما أُحْكِمَ إغلاقُ طرف الماصّة؛ فإنّ ضغطَ الهواء زاد في داخلها؛ ما جعلها قويّة بدرجة كافية لاختراق درنة البطاطس بنجاح.

المراجع
/www.sci-ma.info/category
منوعات/تجارب- وأنشطة- تجارب/
ar.wikipedia.org/wiki/بطاطس


شكل (١) .


شكل (٢) .


شكل (٣).


شكل (٤) .

:: الجديد في العلوم والتقنية ::

رُبع الأسماك الغضروفيّة في العالم على وشك الانقراض

أشارتْ دراسةٌ حديثةٌ قام بها باحثون من الاتّحاد الدُّوَليّ لحماية الطّبيعة (The international Union for Conservation of Nature – IUCN) بالتّعاون مع زملائهم في مركز اختصاصيّ أسماك القرش وجامعة سيمون فريزر بكندا إلى أنّ رُبُع الأسماك الغضروفيّة في العالم –تشمل أسماكَ القرش(Sharks) والشفانين (Rays)– على وشك الانقراض.

مِنْ جانب آخرَ أفادت الدّراسات السّابقة التي وثّقت استمرار الصّيد الجائر لأسماك القرش والشفانين؛ وعليه طبّق الباحثون لائحة الحيوانات المعرَّضة لخطر الانقراض على جميع أنواع الأسماك الغضروفيّة البالغ عددُها ١٠٤١ نوعًا من خلال ١٧ ورشةَ عمل ضمّت نحو ٣٠٠ خبير عالميّ؛ إذ مُسِحَتْ– لأوّل مرّة– المناطقُ الشّاطئيّة والسّاحليّة للبحار والمحيطات، وجمعت المعلومات المتعلّقة بالأسماك الغضروفيّة كافّة، التي تتضمّن التاريخ، والتّوزيع الجغرافيّ، وتوفّر الأعداد لكلّ نوع، والمخاطر التي تواجهها الأسماك الغضروفيّة، وقد خَلص العلماءُ في هذه الدّراسة إلى أنّ ما يُقارب رُبع أنواع الأسماك الغضروفيّة (نحو ٢٤٩ نوعًا من إجماليّ ١٠٤١ نوعًا من أسماك القرش والشفانين) هي على وشك الانقراض، منها ١٨١ نوعًا عند الدّرجة الحمراء من خطر الانقراض (٧٤ نوعًا من أسماك القرش، و ١٠٧ أنواع من الشفانين).

ويشير **نك دولفي (Nick Dulvy)** القائدُ البحثيُّ لهذه الدّراسة مديرُ المركز البحثيّ الكندي للتّنوّع الأحيائي البحريّ قائلًا: (نحن عَلِمْنا الآن أنّ العديدَ من أنواع الأسماك الغضروفيّة تواجَهُ خطرَ الانقراض في العالم، وليس فقط أسماك القرش الأبيض، التي تعيش في العديد من بحار العالم ومحيطاته باستثناء المناطق القطبيّة)، كما يضيف **دولفي** قائلًا: إنّه لا توجد دلائلُ قاطِعَةٌ تُفْصِحُ عنْ درجة أمان أسماك القرش من خطر الصّيد الجائر.

تُعَدُّ أسماكُ القرْش والشفانين معرَّضَةً للانقراض بدرجة عالية موازنة مع العديد من أنواع الحيوانات الأخرى، بالإضافة إلى أنّ لها النّسبةَ الأقلَّ في ناحية الأمان موازنة مع الحيوانات الأخرى. كما توَصّل الباحثون إلى معرفة المناطق التي يكثر فيها تناقصُ أعداد أسماك القرش والشفانين، واتّضح أنّها تشمل: منطقةَ المحيط الهنديّ والهادئ (Indo–Pacific) تحديدًا في خليج تايلاند، إضافة إلى البحر الأحمر والخليج العربيّ.

الجدير بالذّكر أنّ الصّيدَ الجائرَ يحدث لأسماك القرش والشفانين بسبب استخدامها في تصنيع الحساء والمأكولات البحرية (حساء زعانف القرش)؛ ما سيؤثر سلبًا في أعدادها وتعرّضها للانقراض، وبما أنّ أسماكَ القرش تمثّل قمّة الهرم الغذائيّ في النّظام البيئيّ البَحْريّ؛ فإنّه يَسْتَوْجِبُ على صُنّاع القرار اتّخاذُ الإجراءات الصّارمة للحدّ من انقراضَها؛ حفاظًا على الاتّزان البيئيّ.

المصدر

http://www.sciencedaily.com/releases/201 4/01/140122202304.htm

اكتشاف شعاب مَرْجانيّة في جرينلاند

تُعَدُّ الشّعاب المَرْجانيّة من أشْهَر المَعالم السّياحيّة الجاذبة للغوّاصين في العديد من الدُّوَل السّاحليّة في العالم، وقد نَجَحَ باحثون كنديّون بطريق الصّدفة المُطْلَقَة – لأوّل مرّة– في اكتشاف شعاب مَرْجانيّة حيّة في المياه الباردة جنوبَ جرينلاند، كما دَرَست طالبةُ الدكتوراه **هيلي جورجنسباي (Helle Jorgensbye)** من جامعة الدّنمارك للتّقنية هذا المَرجان دراسة مُوَسَّعَة.

تتمركز هذه الشّعاب المَرْجانيّة في الجنوب الغربيّ من جزيرة جرينلاند، وقد تكوّنت من مَرجان الماء البارد (Cold–water corals) التي تمتلك هياكلَ جيريّة قاسِيَة.

تقع الشّعاب المَرْجانيّة المُكْتَشَفَة على عُمْق يَصل إلى قُرابة ٩٠٠ متر في منطقة تكثر فيها التّيّاراتُ البحريّةُ القويّةُ، الأمر الذي يُصّعِبُ معه الوصولُ إليها؛ ما يَدُلُّ على أنّ الشّعابَ المَرْجانيّة في هذه المنطقة لم تُدْرَسْ من قبل؛ لذا فقد اكتشف باحثون كنديّون هذه الشّعاب المَرجانيّة، وغاصوا؛ لتصويرها.

إنّه من المَعْلوم منذ نحو ٨٠٠٠ سنة أنّ الشّعاب المَرجانيّة موجودةٌ في سواحل النرويج وآيسلندا، وقد أُجْرِيَتْ عليها العديدُ من الأبحاث في النّرويج؛ إذ تنمو هناك على ارتفاع يصل إلى ٣٠ مترًا، فيما يبلغ طولُها عدّة كيلومترات، وتشير **جورجنسباي** إلى أنّ الشّعاب المَرجانيّة المُكْتَشَفَة ليست كثيفة كمستعمرات الشّعاب المَرجانية الأخرى المجاورة لجرينلاند، التي تؤثّر في التّيّارات البحريّة التي تَمْتَدّ إلى السّاحل الغربيّ للجزيرة، الذي ترتفع فيه درجةُ حرارة المياه إلى ٤°م، وهي الدّرجة المُناسِبَة لنموّ هذه الشعاب وتكاثرها، بالإضافة إلى وجود التّيّارات المائيّة القويّة؛ مما يُشَكّل ظروفًا مُناسِبَة لنموّها في هذه المنطقة.

تتمثّلُ أهمّيّة الشّعاب المَرْجانيّة في كَوْنها تُمَثّلُ بيئةً مُلائمَةً لحمَاية الأسماك وتغذيتها؛ إذ تمدُّها بالغذاء الوفير والمكان الآمن من المُفْتَرِسات الطّبيعيّة، ويعود مَنْشَأ الشّعاب المَرجانيّة في جرينلاند إلى أحجار لوفيلا (Lophelia) المَرجانيّة، التي يعود اكتشافها إلى العالم الدنماركي **أولي تيندال (Ole Tendal)**، وهناك العديدُ من أنواع المَرجان الأخرى توجدُ غربَ جرينلاند.

الجدير بالذّكر أنّ وجود الشّعاب المَرْجانيّة يرتبط بصورة رئيسة بمياه المناطق الاستوائية؛ إذ تستمدّ طاقتَها ونموَّها من أشعّة الشّمس، إلّا أنّها قد توجد في المياه الباردة؛ إذ تكون مُحاطَة بالظّلام التّامّ، لكنّها تستمدّ طاقتَها من الطّحالب التي توجد عليها؛ لأنّها توجد في أعماق لا تصل إليها الشّمس، كما تَتَشَكّلُ الشّعابُ المَرْجانيّة منْ تَجَمُّع الآلاف من حيوان المَرجان في هيئة مُسْتَعْمَرات مُكَوِّنة الهَيْكَل الجيريّ لها.

:: الجديد في العلوم والتقنية ::

المصدر

Technical University of Denmark (DTU). Note: Materials may be edited for content and length.

http://www.sciencedaily.com/releases/2014/01/140128094334.htm

جينوم الجراد أكبر جينوم في العالم

نَجَحَ باحثون من معهد علم الحيوان التّابع لأكاديمية العلوم في الصين، بالتّعاون معَ معاهدَ أخرى متخصّصة في كشف النّقاب عن شفرة الجينوم الكاملة للجراد المُهاجر (Locusta migratoria) - يُعَدّ أكثر أنواع الجراد انتشارًا في العالم- إذ بلغ طول تتابعات الجينوم ٦,٣ جيجابايت؛ ما يجعله أطول جينوم لكائن حَيٍّ في العالم فُكَّتْ شفرته. يُشير الباحثون إلى أنّ المُفاجَأة التي كُشِفَ عنها في هذه الدّراسة هي أنّ الجرادة الواحدة يمكنها تناولَ غذاء يساوي وزنَها خلال يوم واحد، وهذا ما يوازي تناوُلَ الإنسان كمّيّةً منَ الغذاء توازي ٦٠ ضعفًا من استهلاكه اليوميّ.

يَتَسَبَّبُ الجرادُ المُهاجِرُ بتَلَف المَحاصيل الزراعيّة ودمارها، خاصّة عندما يطير في أسرابه؛ ما يكلّف العديدَ من الدُّوَل مليارات الدولارات. وفي هذه الدراسة تتبّع الباحثون شفرة جينوم الجراد المُهاجر بوساطة تقنية التّتبّع (NEXT-GEN) التي كَشَفَت النّقابَ عن ٧٢١ جيجابايت من البيانات، غطّت مساحةً قدرُها ١١٤ من حجم جينوم الجراد المُهاجر ٦,٣ جيجابايت. كذلك نَجَحَ الباحثون في شَرْح نحو ١٧٣٠٧ نماذجَ من المُوَرِّثات ووصفها، كما نجحوا في تعريف ٢٦٣٩ مُوَرِّثًا مُتَكَرِّرًا، بالإضافة إلى ذلك فقد اكتشفوا أنّ المُوَرِّثات الأولى المُكَرَّرَة تُمثّل ١٠٪ منْ إجماليّ تَسَلْسُل الجينوم.

فَسَّرَ العُلَماءُ سببَ طول الجينوم للجراد المُهاجر موازنَة مع الحشرات الأخرى، وخَلصوا إلى أنّ الجَرادَ المُهاجِر لديه نسبةٌ قليلةٌ منْ مُعدَّل حذف الحمض النوويّ (DNA) ، كما أنّ العناصرَ القابلة للانتقال في الجينوم كبيرة موازنة مع الحشرات الأخرى.

يُمْكِنُ للجراد المُهاجر الطّيَرانُ بسرعة عالية لمسافات طويلة؛ للهجرة وعبور المُحيطات، وقد أماطت هذه الدراسة اللثام عن أن الجراد المهاجر يحفّز معدلات الطاقة لديه عبر المورثات، مِنْ خلال أيض الأحماض الدّهنية، وآليّة إزالة السّموم؛ وذلك لتلبية الاستهلاك المُكثّف للطّاقة طوال مدّى الطّيران لمسافات طويلة، كما يعود سببُ قوّة تكيّف الجراد المُهاجر مع البيئات الصحراوية إلى توسُّع مُسْتقْبلات مُوَرِّثات حاسّتي: التذوّق والشّمّ، وتضخّمها.

الجديرُ بالذّكر أنّه لتطوير مُبيدات حشريّة فعّالة كشف الباحثون في هذه الدّراسة النّقاب عن المُوَرَّثات المُسْتَهْدَفة؛ للتّحَكُّم في الاستجابة للمُبيدات الحشريّة، مثل (cys-loop ligand-gated ion channels) والمُوَرِّث (protein-coupled receptors) التي تُعَدُّ مُوَرِّثات مُسْتَهْدَفة مُهِمّة ستُمَكِّن علماء الحشرات مِنْ تصنيع مُبيدات حشريّة فعّالة في مُواجهة الجَراد المُهاجِر.

المصدر

http://www.sciencedaily.com/releases/2014/01/140116113556.htm

عَلاقةُ مُدّة النّوْم بالاكتئاب

أجرى باحثون مِنْ جامعة واشنطن، سياتل، الولايات المُتّحدة، دراسَتَيْن حديثتين؛ لدراسة العلاقة بين مُدّة النوم والإصابة بالاكتئاب؛ وذلك في التّوائم البالغين. أوْضحت الدّراسة الأولى التي أُجْرِيَتْ على ١٧٨٨ توأمًا -تُعَدُّ الدّراسةَ الأولى مِنْ نوعها- نوعيَّةَ المُورِّث الذي يُرْبطُ بين عادات النّوم وأعراض الاكتئاب، أمّا الدراسة الأخرى التي شملت ٤١٧٥ فردًا -أعمارُهم بين ١١ و ١٧ عامًا- فهي أيضًا الدّراسة الأولى من نوعها، وقد كَشَفَتْ عن وجود علاقة بين الاكتئاب والنّوم القصير في البالغين.

يُشيْرُ الأستاذُ **صفوان بدر (Safwan Badr)** رئيسُ الجَمعيّة الأمريكيّة لِطبّ النّوم قائلًا: إنّ النّوم مُهِمٌّ للصّحّة البدنيّة والنفسيّة والعاطفيّة للإنسان، وقد أثبتت هذه الدّراسةُ الجديدةُ أنّه يُمْكِنُنا استثمارُ صحّتنا؛ بإعطاء ساعات النّوم أوْلَويّة قُصْوَى في حياتنا.

كَشَفَتْ نتائجُ الدّراسة الأولى عن وجود عَلاقة قويّة بين زيادة ساعات النّوم عن الحدّ الطبيعيّ وزيادة المخاطر الوراثيّة لظهور أعراض الاكتئاب؛ ففي حالة التوائم الذين نالوا قسطًا كافيًا من النوم (بين ٧ إلى ٨ ساعات) يوميًا، بلغت نسبة الإصابة بأعراض الاكتئاب ٢٧٪، في حين ازداد مُعَدَّل ظهور أعراض الاكتئاب إلى ٥٣٪ لدى التوائم الذين لم يناموا ساعات كافية (٥ ساعات كلّ ليلة) موازنة مع نسبة ٤٩٪ في الأشخاص الذين ينامون ١٠ ساعات كلّ ليلة.

تشيرُ **ناثانيل واتسون (Nathaniel Watson)** الأستاذُ المُساعدُ في علم الأعصاب بجامعة واشنطن إلى أنّ نتائج الدّراسة كانت مُفاجئة؛ إذ أوْضَحَتْ أنّ حالات توريث أعراض الاكتئاب في التوائم الذين يعانون من قصر ساعات النوم كانت ضِعْف الحالات في التوائم الذين نالوا قسْطًا جيّدًا من النَّوْم. ويُضيْفُ **واتسون** قائلًا: إنّ كلا أوقات النّوم القصيرة والطّويلة تَعْمَلُ على تفعيل دور المُوَرِّثات المُتَعَلِّقة بأعراض الاكتئاب.

أمّا في الدّراسة الثّانية فقد اُخْتُبِرَ تأثيرُ نَقْص ساعات النَّوم على ظهور الاكتئاب من خلال الحصول على معلومات إحصائية من المُشاركين. أوْضَحَت النّتائجُ أنّ المُشاركين الذين ناموا ست ساعات كلّ ليلة زاد لديهم خطر الإصابة بالاكتئاب موازنةً مع باقي المُشاركين، كما كَشَفَتْ نتائجُ هذه الدّراسة أنّ الحِرْمان من النَّوْم يُعَدُّ عاملًا رئيسًا في ظُهور أعْراض الاكتئاب على البالغين، وذلك قبل ظهور الأعراض المَرَضيَّة الأخرى.

أفادت هذه الدراسة أيضًا في مَعْرِفة أنّ أهمّيّة ضَبْط ساعات النوم وموازنتها قد تكون علاجًا فعّالًا لزيادة فَعَاليّة مُضادّات الاكتئاب؛ ما يَسْتَوْجِبُ الاهتمامَ بساعاتِ نوم كافية كلّ ليلة.

المصدر

http://www.sciencedaily.com/releases/2014/01/140131230851.htm



nature
الطبعة العربية
عام واحد..
عشر قصص
أبطال الأخبار العلمية
لعام 2013 صفحة 35
فطر يهدد أفضل
أنواع الموز
إقرأ في العدد السابع عشر
من مجلة نيتشر الطبعة العربية
• فقدان التواصل البصري المبكر بالتوحد.
• خريطة لمخزون العالم من المعادن النادرة.
• تحت البركان.
• أبطال رقميون، و عوالم من صنع الحاسب.
وغيرها عن آخر المستجدات العلمية.



اقرأ في العدد السابع من مجلة العلوم والتقنية للفتيان

- التربينات المائية: ساعة الخيار.
- غرائب الأرض.
- المناخ هو السبب الأول للنزوح السكاني.
- للمحافظة على الصحة: ٥ رياضات بوصفة طبية.
- وحوش البحار.

وغير ذلك من المقالات المشوقة والصور الجميلة.

تصفح هذه المجلة، وجميع إصدارات مدينة الملك عبدالعزيز للعلوم والتقنية على الموقع الإلكتروني
http://publications.kacst.edu.sa



مطابع مدينة الملك عبدالعزيز للعلوم والتقنية
الرقم 340517
رقم الوثيقة: 05P0007-MAG-0020-AR01
http://stm.kacst.edu.sa